ЭЛЕМЕНТЫ МАТЕМАТИКИ

Н. БУРБАКИ

АЛГЕБРА

МОДУЛИ, КОЛЬЦА, ФОРМЫ

ПЕРЕВОД С ФРАНЦУЗСКОГО
Г. В. ДОРОФЕЕВА

ПОД РЕДАКЦИЕЙ
Ю. И. МАНИНА

ИЗДАТЕЛЬСТВО «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1966

517.1
Б 91
УДК 512.8

2-2-3
71-66

ОГЛАВЛЕНИЕ

Глава VII. Модули над кольцами главных идеалов 11

§ 1. Кольца главных идеалов 11

1. Определение кольца главных идеалов 11
2. Делимость в кольцах главных идеалов 12
3. Разложение на экстремальные элементы в кольцах главных идеалов 15
4. Делимость целых рациональных чисел 16
5. Делимость многочленов от одного переменного над полем . 17

§ 2. Модули кручения над кольцом главных идеалов 26

1. Модули кручения 26
2. Каноническое разложение модуля кручения над кольцом главных идеалов 27
3. Применения: I. Каноническое разложение рациональных чисел и рациональных дробей от одного переменного . . . 31
4. Применения: II. Мультипликативная группа целых чисел по mod a 33

§ 3. Свободные модули над кольцом главных идеалов 42

§ 4. Модули конечного типа над кольцом главных идеалов 46

1. Конечные прямые суммы моногенных модулей 46
2. Инвариантные факторы подмодуля 50
3. Структура модулей конечного типа 53
4. Вычисление инвариантных факторов 55
5. Линейные отображения свободных модулей и матрицы над кольцом главных идеалов 56
6. Абелевы группы конечного типа 58
7. Неразложимые модули. Элементарные делители 59

§ 5. Эндоморфизмы векторных пространств 71

1. Модуль, ассоциированный с эндоморфизмом 71
2. Эндоморфизмы векторных пространств над алгебраически замкнутым полем 76
3. Собственные значения и собственные векторы 79
4. Приведение к диагональному виду 83
5. Свойства характеристического многочлена; след и определитель 87

6. Характеристический многочлен тензорного произведения двух эндоморфизмов 90
7. Применение: Нормальный базис циклического расширения 91

Приложение. Эндоморфизмы унитарных модулей 101

1. Модуль, ассоциированный с эндоморфизмом 101
2. Подобные эндоморфизмы 103
3. Применение к эндоморфизмам векторных пространств . . 105

Исторический очерк к главам VI и VII 108

Библиография 117

Глава VIII. Полупростые модули и кольца 119

§ 1. Коммутирование 119
1. Проектирования 119
2. Коммутант и бикоммутант 122
3. Прямые множители и бикоммутанты 124
4. Предварительные замечания о коммутировании в изотипных модулях 127
5. Коммутирование в изотипных модулях 129
§ 2. Артиновы и нетеровы модули 136
1. Артиновы и нетеровы модули 136
2. Разложение модуля конечной длины на неразложимые модули 138
3. Артиновы и нетеровы кольца 141
§ 3. Простые и полупростые модули 146
1. Простые модули 146
2. Классы простых модулей 149
3. Полупростые модули 149
4. Изотипные компоненты полупростых модулей 151
5. Длина полупростых модулей 153
§ 4. Коммутант и бикоммутант полупростого модуля 157
1. Бикоммутант полупростого модуля 157
2. Теорема плотности 158
3. Коммутант простого модуля 160
4. Коммутант полупростого модуля 162
5. Применения: Устойчивые подмодули тензорных произведений 163
§ 5. Простые и полупростые кольца 167
1. Полупростые кольца 167
2. Простые кольца 169
3. Простые компоненты полупростого кольца 170
4. Строение простых колец 171
5. Полупростые подалгебры полупростых алгебр 173
6. Степени, высоты, индексы 175
§ 6. Радикал 185
1. Произведения идеалов 185
2. Радикал модуля 187

3. Радикал кольца 190
4. Радикал артинова кольца и артинова модуля 195
5. Модули над артиновым кольцом 197
§ 7. Радикал и полупростота тензорных произведений 208
1. Предварительные замечания 208
2. Расширение скаляров и радикал 210
3. Тензорное произведение полей 214
4. Тензорное произведение полупростых модулей 216
5. Сепарабельные модули и алгебры 221
6. Тензорное произведение с сепарабельным модулем 223
7. Простые модули над тензорным произведением алгебр . . . 225
§ 8. Применения: I. Композиции расширений 232
§ 9. Применения: II. Полупростые семейства эндоморфизмов векторного пространства 237
1. Полупростые семейства эндоморфизмов векторного пространства 237
2. Абсолютно полупростые семейства эндоморфизмов векторного пространства 238
3. Диагонализируемые семейства эндоморфизмов векторного пространства 241
4. Полупростые и нильпотентные компоненты эндоморфизма 242
§ 10. Простые подкольца. Изоморфизмы простых колец 245
1. Теорема Сколема — Нетер 245
2. Простые подкольца простых колец 247
3. Подполя простых колец 250
4. Группа Брауэра 252
5. Нейтрализующие поля 254
§ 11. Применения 266
1. Конечные тела 266
2. Характеризация тел кватернионов 266
§ 12. Нормы и следы 272
1. Норма и след относительно модуля 272
2. Норма и след в алгебре 276
3. Приведенные норма и след 283
§ 13. Линейные представления 294
1. Линейные представления алгебр 294
2. Матричные представления 296
3. Коэффициенты представлений 297
4. Расширение основного поля линейного представления . . . 300
5. Норма и след относительно представления 302

Приложение. Алгебры без единицы 305

1. Регулярные идеалы 305
2. Простые модули 308
3. Радикал 309

Исторический очерк к главе VIII 314

Библиография 322

Глава IX. Полуторалинейные и квадратичные формы 325

§ 1. Полуторалинейные формы 325
1. Билинейные отображения 325
2. Полуторалинейные отображения 328
3. Ортогональность. Прямые суммы билинейных и полуторалинейных отображений 330
4. Замена основных колец 332
5. Некоторые тождества 337
6. Билинейные и полуторалинейные формы. Ранг 337
7. Обратная форма для билинейной и полуторалинейной форм 342
8. Сопряженный гомоморфизм 344
9. Тензорные произведения и внешние степени полуторалинейных форм 347
10. Матричное исчисление 352
§ 2. Дискриминант полуторалинейной формы 363
§ 3. Эрмитовы и квадратичные формы 371
1. Эрмитовы и ε-эрмитовы формы 372
2. Модули над квадратичным расширением 374
3. Билинейные формы, ассоциированные с эрмитовой формой 375
4. Квадратичные формы 377
§ 4. Вполне изотропные подпространства. Теорема Витта 387
1. Изотропные подпространства 387
2. Разложение Витта 389
3. Теорема Витта 396
§ 5. Некоторые свойства знакопеременных билинейных форм 405
1. Приведение знакопеременных билинейных форм 405
2. Пфаффиан знакопеременной матрицы 408
3. Симплектическая группа 410
§ 6. Некоторые свойства эрмитовых форм 417
1. Ортогональные базисы 417
2. Унитарная группа и ортогональная группа 421
3. Ортогональные проектирования и инволюции 423
4. Симметрии в ортогональной группе 425
5. Группа подобий 426
6. Эрмитова геометрия 428
§ 7. Эрмитовы формы и упорядоченные поля 445
1. Положительные эрмитовы формы 445
2. Закон инерции 448
3. Приведение формы по отношению к данной положительной эрмитовой форме 449
§ 8. Типы квадратичных форм 466
1. Типы квадратичных форм 466

2. Группа типов квадратичных форм 468
3. Кольцо типов квадратичных форм 470
§ 9. Алгебры Клиффорда 472
1. Определение и универсальное свойство алгебры Клиффорда 473
2. Некоторые операции в тензорной алгебре 475
3. Базис алгебры Клиффорда 477
4. Структура алгебры Клиффорда 480
5. Группа Клиффорда 485
§ 10. Углы 496
1. Прямые подобия в плоскости 496
2. Плоская тригонометрия 501
3. Углы 503
4. Угловые секторы 510

Исторический очерк к главе IX 524

Библиография 539

Указатель обозначений 542

Указатель терминов 544

Определения к главе VII . . . . . Вклейка № 1

Определения к главе VIII . . . . . Вклейка № 2

Определения к главе IX . . . . . Вклейка № 3

ГЛАВА VII

МОДУЛИ НАД КОЛЬЦАМИ ГЛАВНЫХ ИДЕАЛОВ

Если не оговорено противное, все кольца, рассматриваемые в этой главе, предполагаются коммутативными и имеющими единицу, а модули — унитарными.

§ 1. Кольца главных идеалов

1. Определение кольца главных идеалов

Определение 1. *Кольцо A называется кольцом главных идеалов, если оно является кольцом целостности* (гл. I, § 8, n° 3, определение 3) *с единицей и всякий его идеал — главный.*

Примеры. Кольцо $\boldsymbol{Z}$ целых рациональных чисел является кольцом главных идеалов (гл. I, § 8, n° 5, пример 4). Кольцо $K[X]$ многочленов от одного переменного над полем K является кольцом главных идеалов (гл. V, IV, § 1, n° 5, предложение 7); таковым же будет и кольцо $K[[X]]$ формальных степенных рядов, так как всякий идеал этого кольца имеет вид (X^n) (гл. IV, § 5, n° 7). Кольцо целых p-адических чисел является кольцом главных идеалов.

Пусть $\boldsymbol{Q}(i)$ — поле, полученное из поля $\boldsymbol{Q}$ рациональных чисел присоединением корня i неприводимого многочлена X^2+1. Элементы этого поля $a+bi$, где a и b — целые рациональные числа, образуют подкольцо A поля $\boldsymbol{Q}(i)$, называемое «кольцом целых гауссовых чисел» и являющееся кольцом главных идеалов (упражнение 7).

Напротив, в поле $\boldsymbol{Q}(\varrho)$, где ϱ — корень многочлена X^2+5, подкольцо B, составленное из элементов вида $a+b\varrho$ (a и b — целые рациональные), не будет кольцом главных идеалов.

Кольцо $K[X, Y]$ многочленов от двух переменных над полем K не является кольцом главных идеалов, так как только ненулевые константы делят одновременно X и Y, но ни одна из них не будет образующей идеала, порожденного X и Y.

2. Делимость в кольцах главных идеалов

Пусть A — кольцо главных идеалов, K — его поле дробей; ранее мы видели, что упорядоченная группа $\mathfrak{F}^*$ главных дробных идеалов (гл. VI, § 1, n° 5) поля K решеточно упорядочена. Более точно:

Предложение 1. *Пусть K — поле дробей кольца главных идеалов A и $(x_\iota)_{\iota\in I}$ — семейство элементов K с общим знаменателем $b \in K^*$ (то есть $bx_\iota \in A$ при любом ι). Тогда:*

1) *Семейство (x_ι) имеет н. о. д. в K.*

2) *Всякий н.о.д. семейства (x_ι) имеет вид $d = \sum_\iota a_\iota x_\iota$, где a_ι — элементы кольца A, причем лишь конечное число их отлично от нуля.*

Действительно, идеал $\sum_\iota A bx_\iota$ кольца A — главный и, следовательно, имеет вид Ad'. Положим $d' = bd$. Из равенства $d' = \sum_\iota a_\iota bx_\iota$ следует $d = \sum_\iota a_\iota b_\iota$, так что всякий общий делитель элементов x_ι делит d. С другой стороны, bd, очевидно, общий делитель элементов bx_ι, и поэтому d является общим делителем элементов x_ι, что и требовалось доказать.

Замечание. Предложение 1 применимо также к любому семейству (x_ι) элементов кольца A (достаточно взять $b = 1$), а также к любому *конечному* семейству (x_ι) элементов K (в самом деле, если $x_\iota = c_\iota b_\iota^{-1}$, $c_\iota \in A$, $b_\iota \in A$, то в качестве b достаточно взять произведение всех b_ι).

Следствие. *Пусть (x_ι) — произвольное семейство элементов в подкольце главных идеалов A кольца целостности и d — н. о. д. этого семейства в A. Тогда семейство (x_ι) обладает н. о. д. в B и d является одним из этих н. о. д.*

В самом деле, d является общим делителем элементов x_ι в B. С другой стороны, равенство $d = \sum_\iota a_\iota x_\iota$ ($a_\iota \in A$) показывает, что всякий общий делитель элементов x_ι в B делит d.

Важным применением этого следствия является тот случай, когда $A = K[X]$, $B = E[X]$, где K — некоторое поле, E — его расширение.

Первое утверждение предложения 1 означает, что группа $\mathfrak{F}^*$ *решеточно упорядочена* (гл. VI, § 1, n° 9). В частности, всякое конечное семейство элементов поля K обладает н. о. к. Следовательно, к кольцам главных идеалов можно применять результаты гл. VI, n°n° 9, 10, 11 и 12, отмеченные знаком (ДЕЛ).

Из второго утверждения предложения 1 следует

Теорема 1 («тождество Безу»). *Для того чтобы элементы* x_ι ($\iota \in I$) *кольца главных идеалов* A *были в совокупности независимы, необходимо и достаточно, чтобы существовали такие элементы* a_ι ($\iota \in I$) *кольца* A, *что* $\sum_\iota a_\iota x_\iota = 1$, *причем лишь конечное число* a_ι *отлично от нуля.*

Необходимость этого условия следует из предложения 1. Обратно, если $\sum_\iota a_\iota x_\iota = 1$, то всякий общий делитель элементов x_ι делит 1, и следовательно, 1 — н. о. д. этих элементов.

Предложение 2. *Пусть* a, b, d, m *и* p — *элементы поля дробей* K *кольца главных идеалов* A. *Тогда следующие утверждения равносильны:*

1) «d — *н. о. д. элементов* a *и* b» *и* «$(d) = (a) + (b)$».

2) «m — *н. о. к. элементов* a *и* b» *и* «$(m) = (a) \cap (b)$».

3) «p — *экстремальный элемент* A» *и* «(p) — *максимальный идеал* A».

Утверждение 1) уже доказано (предложение 1). Далее, общие кратные элементов a и b образуют идеал $(a) \cap (b)$, который, по предположению, является главным идеалом (m), то есть m — н. о. к. элементов a и b. Это доказывает утверждение 2). Наконец, первое из утверждений 3), по определению (гл. VI, § 1, n° 13), равносильно утверждению, что (p) — максимальный элемент упорядоченного по включению множества отличных от A главных идеалов кольца A. Так как все идеалы кольца A — главные, это означает, что (p) — максимальный идеал кольца A, откуда следует 3).

Сумму (соответственно пересечение) конечного числа идеалов кольца главных идеалов A называют иногда н. о. д. (соответственно н. о. к.) этих идеалов.

Предложение 3. *Пусть* a, b, c — *элементы поля дробей кольца главных идеалов* A *и* d — *н. о. д. элементов* a *и* c. *Сравнение*

$ax \equiv b \pmod{c}$ имеет целое решение $x_0 \in A$ тогда и только тогда, когда d делит b; в этом случае все целые решения $x \in A$ этого сравнения совпадают с целыми решениями сравнения $x \equiv x_0 \pmod{cd^{-1}}$.

Если $ax \equiv b \pmod{c}$ и $x \in A$, то существует такой элемент $y \in A$, что $b = ax + cy$. Следовательно, d делит b. Обратно, если d делит b, то $b = ax_0 + cy_0$, где $x_0, y_0 \in A$ (предложение 1). Поэтому $ax_0 \equiv b \pmod{c}$. Кроме того, в этом случае сравнение $ax \equiv b \pmod{c}$ равносильно сравнению $a(x - x_0) \equiv 0 \pmod{c}$; положив $a = da'$ и $c = dc'$, получим $a'(x - x_0) \equiv 0 \pmod{c'}$. Но это сравнение (для всех $x \in A$) равносильно сравнению $x - x_0 \equiv 0 \pmod{c'}$, так как a' и c' — независимые целые элементы (гл. VI, § 1, предложение 10 (ДЕЛ) и следствие 1 предложения 11 (ДЕЛ)).

Предложение 4. *Пусть $(a_i)_{1 \leqslant i \leqslant n}$ — конечное семейство попарно независимых элементов кольца главных идеалов A. Тогда факторкольцо* (соответственно *A-модуль*) $A/(\prod_{i=1}^{n} a_i)$ *изоморфно* (соответственно *изоморфен*) *произведению колец* (соответственно *A-модулей*) $A/(a_i)$.

Так как элемент a_n не зависит от $a_1, \ldots, a_{n-1}$ (гл. VI, § 1, n° 12, следствие 3 предложения 11 (ДЕЛ)), то индукцией по n доказательство сводится к случаю $n = 2$.

Пусть a и b — независимые элементы кольца A. Тогда $(a) + (b) = A$ и $(a) \cap (b) = (ab)$ (гл. VI, § 1, n° 12, предложение 12 (ДЕЛ)). Пусть g (соответственно h) — каноническое отображение кольца A на $A/(a)$ (соответственно на $A/(b)$). Рассмотрим отображение $f = (g, h)$ кольца A в $(A/(a)) \times (A/(b))$. Ясно, что f — гомоморфизм (структуры кольца и структуры A-модуля) и его ядро равно $(a) \cap (b) = (ab)$. Поэтому достаточно показать, что f является отображением кольца A «на» $(A/(a)) \times (A/(b))$, то есть для произвольных элементов c и d кольца A нужно доказать существование такого элемента $x \in A$, что $x \equiv c \pmod{a}$, $x \equiv d \pmod{b}$. Но в силу независимости элементов a и b существуют элементы $u, v \in A$, удовлетворяющие условию $ua + vb = 1$. Поэтому достаточно положить $x = dua + cvb$.

Заключение предложения 4 неверно без предположения о попарной независимости элементов a_i (см. § 4, предложение 6).

3. *Разложение на экстремальные элементы в кольцах главных идеалов*

Теперь мы применим к кольцам главных идеалов результаты гл. VI, § 1, n° 13, относящиеся к разложению на экстремальные элементы. По предложению 2 элемент p кольца главных идеалов A экстремален тогда и только тогда, когда кольцо $A/(p)$ является полем (гл. I, § 9, n° 3, теорема 2), то есть сравнение $ax \equiv b \pmod{p}$ имеет в A решение при любых a и b, не кратных p.

Определение 2. *Системой представителей экстремальных элементов кольца главных идеалов A называется такое семейство (p_α) экстремальных элементов, что всякий экстремальный элемент кольца A ассоциирован с одним и только одним p_α.*

Теорема 2. *Пусть A — кольцо главных идеалов и (p_α) — система представителей его экстремальных элементов. Тогда всякий ненулевой элемент x поля дробей кольца A имеет единственное представление вида*

$$x = u \prod_\alpha p_\alpha^{n_\alpha}, \tag{1}$$

где u — обратимый элемент кольца A, n_α — целые рациональные числа, из которых лишь конечное число отлично от нуля. Для того чтобы элемент x был целым, необходимо и достаточно, чтобы все n_α были положительными.

Для доказательства применим теорему о разложении в сумму экстремальных элементов (гл. VI, § 1, теорема 2 и предложение 15), наше утверждение, по существу, является ее перефразировкой. Так как группа $\mathfrak{F}^*$ решеточно упорядочена, условия упомянутой теоремы будут выполнены, если мы убедимся в том, что всякое непустое множество главных идеалов кольца A имеет максимальный элемент; но это следует из леммы:

Лемма. *Пусть A — кольцо* (быть может, некоммутативное и без единицы), *в котором всякий левый идеал имеет конечное число образующих. Тогда всякое непустое множество Φ левых идеалов кольца A, упорядоченное по включению, имеет максимальный элемент.*

В силу теоремы Цорна (Теор. мн., Рез., § 6, n° 10) достаточно доказать, что множество Φ индуктивно. Если (a_λ) — совершенно

упорядоченное множество элементов Ф, то объединение $\mathfrak{a}$ идеалов $\mathfrak{a}_\lambda$ является левым идеалом кольца A и имеет, следовательно, конечное число образующих $(a_i)_{1\leqslant i\leqslant n}$. Но всякий элемент a_i принадлежит некоторому идеалу $\mathfrak{a}_{\lambda_i}$, и так как множество $(\mathfrak{a}_\lambda)$ совершенно упорядочено, то все a_i $(1\leqslant i\leqslant n)$ входят в наибольший из идеалов $\mathfrak{a}_{\lambda_i}$, скажем $\mathfrak{a}_\mu$. Тогда $\mathfrak{a}=\mathfrak{a}_\mu$ принадлежит Ф, то есть множество Ф индуктивно.

В дальнейшем мы будем изучать *нетеровы кольца*, то есть коммутативные кольца, в которых каждое непустое множество идеалов имеет максимальный элемент.

Замечание. Правая часть равенства (1) называется разложением элемента x на экстремальные множители. Если $x=u\prod_\alpha p_\alpha^{n_\alpha}$ и $y=v\prod_\alpha p_\alpha^{m_\alpha}$ — разложения элементов x и y на экстремальные множители, то x делит y тогда и только тогда, когда для всякого α $n_\alpha\leqslant m_\alpha$; отсюда

$$\text{н. о. д. } (x, y)=\prod_\alpha p_\alpha^{\inf(n_\alpha, m_\alpha)}, \tag{2}$$

$$\text{н. о. к. } (x, y)=\prod_\alpha p_\alpha^{\sup(n_\alpha, m_\alpha)}. \tag{3}$$

Свойство, описываемое теоремой 2, справедливо для колец более широкого класса; эти кольца появятся у нас ниже под названием *факториальных колец*. Мы увидим, что кольца многочленов и формальных степенных рядов от любого числа переменных являются факториальными кольцами.

4. *Делимость целых рациональных чисел*

Как было сказано, кольцо $\boldsymbol{Z}$ целых рациональных чисел является кольцом главных идеалов; его поле дробей есть $\boldsymbol{Q}$. Мультипликативная группа U обратимых элементов кольца $\boldsymbol{Z}$ состоит из двух элементов: 1 и —1. Группа $\boldsymbol{Q}_+^*$ строго положительных рациональных чисел содержит единственный элемент из каждого класса ассоциированных элементов кольца Q; следовательно, она изоморфна группе $\mathfrak{F}^*=\boldsymbol{Q}^*/U$ главных дробных идеалов поля $\boldsymbol{Q}$, с которой ее обычно и отождествляют. В дальнейшем, когда речь будет о н. о. д. или н. о. к. в поле $\boldsymbol{Q}$ (относительно кольца $\boldsymbol{Z}$), будет предполагаться, что эти элементы $\geqslant 0$; это

позволит говорить о единственных н. о. д. и н. о. к. некоторого множества рациональных чисел.

Экстремальные целые числа >0 кольца $\boldsymbol{Z}$ — это в точности числа, которые мы называем *простыми рациональными числами* или, короче, *простыми числами* (гл. I, § 8, n° 7); таким образом, всякий экстремальный элемент кольца $\boldsymbol{Z}$ имеет вид p или $-p$, где p — простое число, и множество простых чисел является системой экстремальных представителей элементов кольца $\boldsymbol{Z}$.

Предложение 5. *Множество простых чисел бесконечно.*

В самом деле, если (p_i) $(1 \leqslant i \leqslant n)$ — произвольное конечное семейство различных простых чисел, то любой простой делитель q числа $(\prod_{i=1}^{n} p_i) + 1$, больший 1, отличен от всех p_i, так как в противоположном случае он делил бы 1.

5. *Делимость многочленов от одного переменного над полем*

Кольцо $K[X]$ многочленов от одного переменного над полем K является кольцом главных идеалов (гл. IV, § 1, n° 5, предложение 7). Его поле дробей есть поле $K(X)$ рациональных функций от X с коэффициентами из поля K. Кольцо $K[X]$ содержит подкольцо многочленов нулевой степени, то есть поле констант, которое обычно отождествляется с K; элементы, входящие в K^*, обратимы в K, а следовательно, и в $K[X]$; обратно, из равенства $\deg(uv) = \deg u + \deg v$ следует, что всякий обратимый многочлен из $K[X]$ имеет нулевую степень; поэтому группа U обратимых элементов кольца $K[X]$ совпадает с K^*. Таким образом, два ассоциированных многочлена отличаются друг от друга только ненулевым постоянным множителем; в частности, всякий класс ассоциированных многочленов содержит единственный *унитарный* многочлен (гл. IV, § 16, n° 3). Следовательно, подгруппа, порожденная в $K(X)^*$ унитарными многочленами, содержит ровно по одному элементу из каждого класса ассоциированных рациональных дробей и поэтому изоморфна группе $\mathfrak{F}^* = K(X)^*/U$ главных дробных идеалов поля $K(X)$. В частности, всякий раз, когда будет идти речь о н. о. д. или н. о. к. в поле $K(X)$ (относительно кольца $K[X]$), будет предполагаться, что эти элементы

являются частными унитарных многочленов (или нулем). Благодаря этому соглашению можно говорить о вполне определенных н. о. д. и н. о. к. любого множества рациональных дробей.

Экстремальными элементами кольца $K[X]$ являются *неприводимые многочлены* (гл. IV, § 1, n° 4, определение 4), а множество I неприводимых унитарных многочленов является системой представителей экстремальных элементов кольца $K[X]$.

Многочлен первой степени всегда неприводим. Если поле K алгебраически замкнуто, то верно и обратное (гл. V, § 4, n° 2, предложение 1); следовательно, в этом случае каждый многочлен $p(X)$ степени n из кольца $K[X]$ может быть единственным образом (с точностью до порядка множителей) представлен в виде

$$p(X) = c(X-a_1)(X-a_2)\dots(X-a_n),$$

где c и a_i — элементы поля K.

Предложение 6. *Для всякого поля K множество унитарных неприводимых многочленов кольца $K[X]$ бесконечно.*

В самом деле, пусть (p_i) $(1 \leqslant i \leqslant n)$ — некоторое непустое семейство различных неприводимых унитарных многочленов; тогда многочлен $\left(\prod_{i=1}^{n} p_i\right) + 1$ необратим и всякий его неприводимый унитарный множитель непременно отличен от всех p_i: в противном случае он делил бы 1.

Упражнения. 1) Показать, что если A — кольцо целостности, то кольцо $A[X_i]$ не может быть кольцом главных идеалов: 1) если число переменных X_i больше или равно 2; 2) если A — не поле (рассмотреть идеалы $(X_\alpha)+(X_\beta)$ $(\alpha \neq \beta)$ и $(a)+(X_\alpha)$, где a — необратимый элемент из A*).

2) Показать, что в кольце $K[[X]]$ формальных степенных рядов над полем K всякий экстремальный элемент ассоциирован с X.

*3) а) Показать, что кольцо целостности, в котором всякий идеал главный и всякое непустое множество идеалов имеет максимальный элемент, есть кольцо главных идеалов (воспользоваться тем, что для всякого идеала a кольца A, не совпадающего с A, существует такой максимальный идеал (p), что $\frac{1}{p}a$ — идеал кольца A, содержащий a и не совпадающий с ним).

б) Пусть K — поле, $K_1 = K[[X]]$ — поле формальных степенных рядов от одного переменного X (гл. IV, § 5, n° 7), $B = K_1[[Y]]$ — кольцо формальных степенных рядов от Y с коэффициентами из поля K_1. Пусть A — подкольцо в B, состоящее из формальных рядов

$\sum_{n=0}^{\infty} a_n (X) Y^n$, у которых формальный ряд $a_0 (X)$ содержит степени X лишь с положительными показателями. Доказать, что главный идеал (X) — единственный максимальный в A, а идеал, порожденный элементами YX^{-n} (n — целое рациональное число), не является главным.

4) Пусть A — кольцо целостности, S — устойчивое относительно умножения множество ненулевых элемеитов этого кольца. Обозначим через A_S кольцо элементов as^{-1} ($a \in A$, $s \in S$) поля дробей K кольца A (гл. I, § 9, упражнение 7).

а) Показать, что если A — кольцо главных идеалов, то и A_S — кольцо главных идеалов.

б) Показать, что если A — кольцо главных идеалов и (p) — его экстремальный элемент, то дополнение S к идеалу (p) устойчиво относительно умножения; показать далее, что идеал pA_S — единственный максимальный идеал кольца A_S и поле A_S/pA_S изоморфно $A/(p)$.

*5) Коммутативное кольцо с единицей называется *квазикольцом главных идеалов*, если всякий его идеал главный.

а) Показать, что факторкольцо квазикольца главных идеалов, а также произведение конечного числа квазиколец главных идеалов являются квазикольцами главных идеалов.

б) Элемент $p \neq 0$ квазикольца главных идеалов A называется *неделимым*, если он необратим, и из равенства $p = xy$ ($x \in A$, $y \in A$) следует, что либо x, либо y принадлежит A_p. Показать, что всякий элемент квазикольца главных идеалов A может быть представлен (по крайней мере одним способом) в виде произведения обратимых и неделимых элементов (применить лемму к теореме 2).

в) Идемпотент e коммутативного кольца A называется *неразложимым*, если не существует пары ненулевых идемпотентов, удовлетворяющей условиям $e = f + g$, $fg = 0$. Показать, что произведение двух неразложимых идемпотентов равно нулю. Показать, что в квазикольце главных идеалов A всякий идемпотент является суммой неразложимых идемпотентов (показать, что если e — идемпотент, то и $1-e$ — идемпотент; применить лемму к теореме 2). Вывести отсюда, что всякое квазикольцо главных идеалов есть прямая композиция конечного множества квазиколец главных идеалов A_i, в каждом из которых единица является неразложимым идемпотентом. Для того чтобы элемент $a = \sum_i a_i$ ($a_i \in A_i$) кольца A был неделимым, необходимо и достаточно, чтобы существовал такой индекс k, что $i \neq k$, элемент a_i был необратим в A_i, а a_k был неделим (в A_k) или равен нулю (последний случай не может осуществиться, если A_k — кольцо целостности). Привести пример неделимого элемента $a \in A$, для которого идеал Aa не является главным максимальным.

*6) Пусть A — квазикольцо главных идеалов (упражнение 5) с делителями нуля, в котором единица является разложимым идемпотентом.

а) Показать, что если для некоторого элемента x кольца A выполняется условие $x^k \in Ax^{k+1}$, то или x обратим, или $x^k = 0$ (если $x^k = ax^{k+1}$, рассмотреть элемент $a^k x^k$).

б) Применив упражнение 5б) и лемму к теореме 2, показать, что существуют неделимый элемент p и конечная последовательность $(a_k)_{1 \leqslant k \leqslant m}$ отличных от нуля элементов кольца A, обладающих свойством $0 = pa_1$, $a_k = pa_{k-1}$ для $1 \leqslant k \leqslant m-1$, $a_m \overline{\in} A_p$ (определить последовательность (a_k) индуктивно и показать, что идеалы Aa_k и Aa_{k-1} различны).

в) Показать, что главный идеал Ab, состоящий из таких $y \in A$, что $yp^m \in Ap^{m+1}$, совпадает с A; применив а), вывести отсюда, что $p^m = 0$.

г) Пусть q — неделимый элемент кольца A; показать, что главный идеал $Ap + Aq$ необходимо совпадает с Ap (заметить, что в противном случае он совпадал бы с A и что, с другой стороны, ввиду в), элемент $1 - xp$ обратим при любом $x \in A$). Вывести отсюда, что Ap — максимальный идеал в A и что всякий элемент, не принадлежащий Ap, обратим (применить упражнение 5б)).

д) Показать, что $q = up$, где u — обратимый элемент (с помощью в) показать, что u не может принадлежать Aq и, следовательно, должны выполняться равенства $p = vq = uvp$; доказать, что элемент uv обратим, установив с помощью а), что главный идеал, состоящий из таких $z \in A$, что $zp \in Ap^2$, совпадает с Ap). Вывести отсюда, что для всякого $x \in A$ существуют целое рациональное число $k \geqslant 0$ и обратимый элемент w такие, что $x = wp^k$, и что единственными идеалами кольца A являются идеалы Ap^k $(0 \leqslant k \leqslant m)$; с помощью а) доказать, кроме того, что эти идеалы различны.

е) Пусть (x_ι) — семейство элементов кольца A, и пусть Ad — порожденный им идеал. Показать, что существуют такие элементы x'_ι, что для всякого ι $x_\iota = dx'_\iota$ и $\sum_\iota Ax'_\iota = A$. Применяя упражнение 5, распространить это утверждение на произвольные квазикольца главных идеалов.

7) Пусть A — кольцо целостности с единицей. Отображение w группы A^* в $\boldsymbol{N}$ называется *евклидовой статмой*, если выполняются следующие условия:

(S_I) $w(xy) \geqslant w(y)$ для любых элементов x, $y \in A^*$.

(S_{II}) Если $a \in A^*$ и $b \in A^*$, то существуют элементы q, r кольца A такие, что выполняется равенство $a = bq + r$, причем $r = 0$ или $w(r) < w(b)$.

Кольцо A называется *евклидовым*, если на нем существует евклидова статма.

а) Показать, что кольца $\boldsymbol{Z}$ и $K[X]$ (где K — поле) евклидовы.

б) Показать, что всякое евклидово кольцо является кольцом главных идеалов (пусть $\mathfrak{a}$ — идеал кольца A; рассмотреть элемент идеала $\mathfrak{a}$ с наименьшим значением $w(a)$).

в) Показать, что кольцо A целых гауссовых чисел евклидово, так как оно обладает статмой $w(a+bi) = a^2+b^2 = N_{Q(i)/Q}(a+bi)$ (установить, что для любого $x \in Q(i)$ существует такой элемент $y \in A$, что $N(x-y) \leqslant \frac{1}{2}$).

г) Показать, что кольцо B, являющееся квадратичным расширением кольца Z с базисом $(1, e)$ $(e^2 = 2)$, евклидово со статмой

$$w(a+be) = |a^2-2b^2| = |N_{Q(e)/Q}(a+be)|$$

(для любого $x \in Q(e)$ существует такой элемент $y \in B$, что $|N(x-y)| \leqslant \frac{1}{2}$).

8) Пусть K — квадратичное поле, то есть расширение степени 2 поля Q.

а) Показать, что $K = Q(e)$, где e^2 — целое рациональное число d, не делящееся ни на какой квадрат (в Z).

б) Пусть $\alpha = a+be$ $(a \in Q,\ b \in Q)$. Обозначим через $\bar{\alpha}$ сопряженный к α элемент $a-be$. Элемент α квадратичного поля K называется целым, если его норма $\alpha\bar{\alpha}$ и его след $\alpha+\bar{\alpha}$ — целые рациональные числа. Показать, что целые числа поля K образуют кольцо A (установить, что если α и β — целые числа поля K, то сумма и произведение рациональных чисел $\alpha\beta+\bar{\alpha}\bar{\beta}$ и $\alpha\bar{\beta}+\beta\bar{\alpha}$ — целые, так что эти рациональные числа являются корнями некоторого унитарного многочлена над Z; вывести отсюда, что они — целые рациональные числа).

в) Показать, что целые элементы поля $K = Q(e)$ образуют Z-модуль с базисом $(1, e)$, если $d-1 \not\equiv 0 \pmod 4$, и $\left(\frac{1}{2}(1+e), \frac{1}{2}(1-e)\right)$, если $d-1 \equiv 0 \pmod 4$; установить, что если $a+be$ — целый элемент поля K, то $2a$ и $2b$ — целые рациональные числа, удовлетворяющие сравнению $2a^2 - d(2b)^2 \equiv 0 \pmod 4$; выяснить, могут ли они быть нечетными). Показать, что дискриминанты этих базисов (гл. V, § 1, n° 6) равны $4d$ и d соответственно.

°9) (Лемма Минковского) Пусть a, b, c, d — действительные числа и $D = \begin{vmatrix} a & b \\ c & d \end{vmatrix}$. Тогда при $AB \geqslant D$ неравенства $|na+mb| \leqslant A$, $|nc+md| \leqslant B$ имеют целые решения (n, m) и этих решений конечное число (рассмотреть в R^2 дискретную подгруппу G, порожденную парами (a, c) и (b, d), и показать, что прямоугольник E, определенный соотношениями $0 \leqslant x \leqslant A$, $0 \leqslant y \leqslant B$, площадь которого больше площади параллелограмма, построенного на векторах (a, c) и (b, d), содержит два различных вектора, конгруэнтных по mod G; рассуждения провести от противного, заметив, что иначе n^2 прямоугольников,

полученных из E с помощью сдвигов ($ha + kb$, $hc + kd$), где $0 \leqslant h < n$, $0 \leqslant k < m$, попарно не пересекались бы).

*10) Пусть d — целое рациональное число, не делящееся на квадрат. Будем рассматривать единицы квадратичного поля $K = Q(\sqrt{d})$, то есть обратимые элементы кольца A целых чисел поля K (упражнение 8б)).

а) Показать, что если $d < 0$ («мнимое квадратичное поле»), то единственными единицами K являются 1 и -1, кроме случаев $d = -1$, когда единицами будут также i и $-i$, и $d = -3$, когда единицами будут еще $\frac{1}{2}(\pm 1 \pm \sqrt{-3})$.

б) Предположим теперь, что $d > 0$ (действительное квадратичное поле) и поле K вложено в некоторое максимальное упорядоченное расширение поля Q (гл. VI, п° 5), °например в R_0. Показать, что положительные единицы образуют подгруппу U' группы U единиц поля K и U есть прямое произведение групп U' и $\{-1, 1\}$.

в) Показать, что единицы поля K целые и имеют норму 1 или -1.

г) Показать, что группа U' не единичная (обозначим через D квадратный корень из дискриминанта базиса целых элементов (упражнение 8в)); показать, что целые элементы поля K, удовлетворяющие условию $N(\alpha) \leqslant D$, разбиваются на конечное число классов по mod U; выбрать в каждом классе целое β_i и для всякого действительного числа B, удовлетворяющего неравенствам $0 < B < \inf(|\beta_i|)$, показать, что (упражнение 9) существует такое целое β, что $0 < \beta \leqslant |B|$ и $N(\beta) \leqslant D$; вывести отсюда, что один из элементов $\beta\beta_i^{-1}$ является единицей η, причем $|\eta| < 1$.

д) Показать, что U' изоморфна Z (доказать существование единицы ε такой, что $|\varepsilon| < 1$, где $|\varepsilon|$ — наибольшее из возможных, используя упражнение 9 и тот факт, что для единицы ξ $|\xi\overline{\xi}| = |\xi|^{-1}$.

е) Показать, что элемент $\sqrt{2}-1$ поля $Q(\sqrt{2})$ является единицей в U' и имеет норму -1.

ж) Вывести из предыдущего, что в случае $d = -1 \not\equiv 0 \pmod 4$ «уравнение Ферма» $a^2 - 2b^2 = 1$ имеет целые решения (в случае, когда d имеет простой делитель вида $4n - 1$, можно показать, что K не имеет единиц с нормой -1; показать на примерах ($d = 2$, $d = 10$), что K может иметь единицы с нормой -1, когда все его нечетные простые делители имеют вид $4n + 1$).

*11) Найти такие квадратичные поля $Q(\sqrt{d})$, для которых отображение $\alpha \to |N(\alpha)|$ является евклидовой статмой (упражнение 7).

а) Показать, что это выполняется тогда и только тогда, когда для любого заданного $\alpha \in Q(\sqrt{d})$ можно найти такое целое число β поля $Q(\sqrt{d})$, что $|N(\alpha - \beta)| < 1$; записать это условие, выразив α и β через базис целых элементов поля (упражнение 8в)).

б) Показать, что в случае мнимого квадратичного поля ($d < 0$) единственные значения d, для которых $|N(\alpha)|$ есть евклидова статма, суть -1, -2, -3, -7, -11.

в) В случае действительного квадратичного поля ограничимся случаями $d \equiv 2$ или $3 \pmod 4$. Показать, что тогда существует только *конечное* число значений d, для которых $|N(\alpha)|$ является евклидовой статмой. (Если $|N(\alpha)|$ — эвклидова статма и a — натуральное число, такое, что $0 \leqslant a \leqslant d$ и $a \equiv t^2 \pmod d$, то, рассмотрев элемент $\frac{1}{\sqrt{d}}$ поля $Q(\sqrt{d})$, показать, что либо a, либо $a - d$ имеют вид $x^2 - dy^2$, где x и y — целые рациональные числа; показать затем, что если d достаточно велико, то можно найти такое нечетное число z, что $5d < z^2 < 6d$ (при $d \equiv 3 \pmod 4$) или $2d < z^2 < 3d$ (при $d \equiv 2 \pmod 4$)); затем взять $a = z^2 - d\,[z^2/d^2]$ и рассматривая остатки по mod 8, показать, что при этих условиях ни a, ни $a - d$ не имеют вида $x^2 - dy^2$.) Показать, что единственные значения d, для которых целое z не существует, суть 3, 7, 11, 19, 23, 35, 47 и 59 (для $d \equiv 3 \pmod 4$) и 2, 6, 14 и 26 (для $d \equiv 2 \pmod 4$). Дать эффективное доказательство существования евклидовой статмы для $d = 2$ и $d = 3$.

12) Показать, что кольцо целых элементов квадратичного поля $Q(\alpha)$, где $\alpha^2 = -5$, не является кольцом главных идеалов (в нем $9 = 3 \cdot 3 = (2 + \alpha)(2 - \alpha)$ и $(1 + \alpha)(1 - \alpha) = 6 = 2 \cdot 3$, и элементы 2, 3, $1 + \alpha$, $1 - \alpha$, $2 + \alpha$, $2 - \alpha$ экстремальные). Показать то же самое для $Q(\beta)$, где $\beta^2 = 10$ ($2 \cdot 3 = (4 + \beta)(4 - \beta)$).

13) Показать, что многочлен $f(x)$ с целыми рациональными коэффициентами, отличный от константы, не может принимать простых значений для всех целых n (рассмотреть $f(n + f(n))$ для таких n, что $f(n) > 1$). Пользуясь идеями доказательства предложения 5, показать, что множество простых чисел, делящих по крайней мере один из членов последовательности $(f(n))$, бесконечно (рассмотреть $f(n + af(n))$ для подходящего a и таких n, что $f(n) \neq 0$).

14) Множество простых чисел вида $4n - 1$ (соответственно $6n - 1$) бесконечно (использовать метод доказательства предложения 5); заметить, что всякое простое число, не равное 2, имеет вид $4n \pm 1$ или $6n \pm 1$).

15) Число вида $2^k + 1$ (k — целое) может быть простым только в случае, когда k есть степень числа 2. Если p—простой делитель числа $2^{2^n} + 1$, то оно не может быть делителем $2^{2^m} + 1$ для $m > n$ ($2^{2^m} \equiv 1 \pmod p$); получить отсюда новое доказательство предложения 5. Показать, что $n = 2^{2^5} + 1$ не простое число (положить $a = 2^7$, $b = 5$; показать, что $1 + ab - b^4 = 24$, и подставить $1 + ab$ в равенство $n = 2^4 a^4 + 1 = (1 + ab - b^4)\, a^4 + 1$).

16) Число вида $a^k - 1$ (a и k — целые, $k > 1$) может быть простым только в случае, когда $a = 2$ и k — простое.

17) Показать, что если $a^n + 1$ — простое число, $a > 1$ и $n > 1$, то a четно и $n = 2^m$.

18) Пусть M — мультипликативный моноид, порожденный конечным числом целых чисел $q_i > 1$ $(1 \leqslant i \leqslant m)$. Показать, что для любого целого числа $k > 0$ существует k последовательных чисел, не принадлежащих M (если $h_1, \ldots, h_m$ — целые числа, большие 1, и k — наибольшее число последовательных чисел, ни одно из которых не делится ни на одно из h_i, то $(k+1)^{-1} = h_1^{-1} + \ldots + h_m^{-1}$, установить затем, что для любого $r > 0$ всякое достаточно большое число из множества M делится по крайней мере на одно из чисел q_i^r). Получить отсюда новое доказательство предложения 5.

19) Доказать, что для любого целого $n > 0$ показатель степени, с которым простое число p входит в $n!$, равен $\sum_{k=1}^{\infty} [np^{-k}]$ (эта сумма имеет лишь конечное число ненулевых членов).

°*20) Пусть $\pi(x)$ — число простых чисел, меньших действительного числа $x > 0$*). Показать, что для любого целого $n > 0$ выполняется неравенство

$$n^{\pi(2n)-\pi(n)} \leqslant \binom{2n}{n} \leqslant (2n)^{\pi(2n)}$$

(установить, что $\binom{2n}{n}$ кратно произведению простых чисел q таких, что $n < q \leqslant 2n$; используя упражнение 19, показать, что, с другой стороны, $\binom{2n}{n}$ делит произведение $\prod p^{r(p)}$, где p пробегает множество простых чисел, меньших или равных $2n$, а $r(p)$ — наибольшее число, для которого $p^{r(p)} \leqslant 2n$). Вывести отсюда существование таких действительных чисел a и b, что $0 < a < b$,

$$an(\log n)^{-1} \leqslant \pi(n) \leqslant bn(\log n)^{-1}$$

(установить, что $2^{2n}n^{-1} \leqslant (2n)!\,(n!)^{-2} \leqslant 2^{2n}$).

21) Показать, что для $m > 1$ и $n > 1$ рациональное число $n^{-1} + (n+1)^{-1} + \ldots + (n+m)^{-1}$ не может быть целым числом (если 2^q — наибольшая степень числа 2, которая делит хотя бы одно из чисел n, $n+1$, $\ldots$, $n+m$, то она делит только одно из них).

22) Пусть a и b — целые числа, большие нуля, d — их н. о. д., n — целое число; положим $a = da_1$, $b = db_1$; показать, что если дробь $a(a+b)\ldots(a+(n-1)b)/n!$ записать в несократимом виде, то ее знаменатель содержит только простые делители числа b_1, не превосходящие n (рассмотреть показатель степени, с которым некоторый простой делитель входит в знаменатель, и применить упражне-

*) Доказано, что при $x \to +\infty$ имеет место асимптотика $\pi(x) \sim x/\log x$ (см., например, И н г а м, Распределение простых чисел, Москва, 1930).

ние 19). Получить отсюда прямое доказательство того, что биномиальные коэффициенты $n!/(m!\,(n-m)!)$ — целые числа.

23) Пусть n — целое рациональное число, большее 1; показать, что н. о. д. $n-1$ биномиальных коэффициентов $\binom{n}{k}$ $(1 \leqslant k \leqslant n-1)$ равен 1, если n делится на два различных простых числа, и равен p, если n есть степень простого числа p.

24) а) Пусть $n = \sum_k p_k^{\nu_k}$ — разложение целого рационального числа на простые множители. Показать, что сумма положительных делителей n равна

$$\sigma(n) = \prod_k \frac{p_k^{\nu_k+1}-1}{p_k-1}.$$

б) Число n называется совершенным, если $2n = \sigma(n)$. Показать, что четное число n совершенно тогда и только тогда, когда оно имеет вид $2^h(2^{h+1}-1)$, где $h \geqslant 1$ и $2^{h+1}-1$ — простое (если n имеет вид $2^m q$, где $m \geqslant 1$ и q — нечетное, то q делится на $2^{m+1}-1$; вывести отсюда, что если бы q не было простым, то выполнялось бы неравенство $\sigma(n) > 2n$).

25) Пусть a и b — независимые строго положительные целые числа. Если a и $b > 2$, то существуют такие целые числа x и y, что $ax + by = 1$ и $|x| < \frac{1}{2}b$, $|y| < \frac{1}{2}a$. Более того, пара чисел x, y, удовлетворяющая этим условиям, единственна. Рассмотреть случай, когда одно из чисел a и b равно 2.

26) Пусть x и y — независимые целые числа; всякое целое число z, такое, что $|z| < |xy|$, может быть одним или двумя способами представлено в виде $z = ux + vy$, где u и v — целые, причем $|u| < |y|$, $|v| < |x|$. Привести пример, в котором z имеет два таких представления.

27) Пусть f и g — независимые многочлены кольца $K[X]$; показать, что всякий многочлен h, такой, что $\deg(h) < \deg(fg)$, может быть единственным образом представлен в виде $h = uf + vg$, где u и v — многочлены, и $\deg(u) < \deg(g)$, $\deg(v) < \deg(f)$. (Провести сначала доказательство, как в упражнении 26 (основанное на алгоритме Евклида), а затем доказательство, в котором задача сводится к линейной.)

*28) а) Пусть K — алгебраически замкнутое поле, f — отличный от константы унитарный многочлен из $K[X]$, g — многочлен из $K[X, Y]$; предположим, что для каждого корня α_i многочлена f существует корень β_i многочлена $g(\alpha_i, Y)$ такой, что $\frac{\partial g}{\partial Y}(\alpha_i, \beta_i) \neq 0$. Показать, что существует многочлен $h(X) \in K[X]$ такой, что $g(X, h(X)) \equiv 0 \pmod{f(X)}$ (с помощью предложения 4 свести

доказательство к случаю $f(X) = X^m$ ($m \geqslant 1$); доказать, что кольцо $K[X]/(X^m)$ изоморфно факторкольцу $K[[X]]/(X^m)$, и применить предложение 10 гл. IV, § 5).

б) Показать, что, в частности, если m — целое число, и делящееся на характеристику поля K, то для любой пары независимых унитарных многочленов f и f_0 из $K[X]$ существует такой многочлен $h(X) \in K[X]$, что $(h(X))^m \equiv f_0(X) \pmod{f(X)}$.

§ 2. Модули кручения над кольцом главных идеалов

1. *Модули кручения*

Пусть M — модуль над коммутативным кольцом A. Будем говорить, что элемент $x \in M$ *аннулируется* элементом $\alpha \in A$, если $\alpha x = 0$ (другими словами, если α принадлежит *аннулятору* элемента x (гл. II, § 1, n° 9)); следовательно, всякий *зависимый* элемент модуля M — это элемент, который аннулируется некоторым *ненулевым* элементом кольца A. Для всякого элемента $\alpha \in A$ множество $M(\alpha)$ аннулируемых им элементов модуля M образует *подмодуль* в модуле M — ядро гомотетии $x \to \alpha x$.

Предложение 1. *Множество M зависимых элементов модуля E над кольцом целостности A является подмодулем модуля E.*

В самом деле, если x и y— зависимые элементы, то существуют такие отличные от нуля элементы α и β, лежащие в A, что $\alpha x = 0$ и $\beta y = 0$. Но тогда $\alpha\beta \neq 0$ и для любых $\lambda, \mu \in A$ $\alpha\beta(\lambda x + \mu y) = 0$, так что элемент $\lambda x + \mu y$ зависимый.

Замечание. Пусть E — модуль над произвольным коммутативным кольцом A. Если $x \in E$ — зависимый элемент, то всякий элемент подмодуля Ax зависим. Но если A имеет делители нуля, то сумма двух зависимых элементов может не быть зависимым элементом: например, в кольце $\mathbf{Z}/(6)$, рассматриваемом как модуль над самим собой, $1 = 3 + 4$.

Предложение 1 приводит к следующему определению:

Определение 1. *Подмодулем кручения модуля E над кольцом целостности называется подмодуль, образованный зависимыми элементами модуля E.*

Если E совпадает со своим подмодулем кручения (то есть всякий его элемент зависим), то, допуская вольность речи, говорят,

что E есть *модуль кручения*. Если подмодуль кручения модуля E нулевой (то есть всякий ненулевой элемент модуля свободен), то E называется *модулем без кручения*.

Предложение 2. *Если M — подмодуль кручения модуля E над кольцом целостности A, то фактормодуль E/M без кручения.*

В самом деле, пусть $\dot{x}$ — класс элемента $x \in E$ по mod M. Если $\dot{x}$ — зависимый элемент фактормодуля E/M, то существует ненулевой элемент $\alpha \in A$ такой, что $\alpha x \in M$; но тогда существует элемент $\beta \in A$, $\beta \neq 0$, такой, что $\beta(\alpha x) = 0$, и так как $\beta\alpha \neq 0$, то $x \in M$.

Ясно, что если M — подмодуль кручения модуля E, то для всякого подмодуля F модуля E пересечение $F \cap M$ является подмодулем кручения модуля F. В частности, всякий подмодуль модуля кручения сам будет модулем кручения. С другой стороны, всякий фактормодуль модуля кручения тоже будет модулем кручения. Наконец, если (M_ι) — произвольное множество модулей кручения над кольцом целостности A, то их прямая сумма M будет модулем кручения. В самом деле, если $x \in M$ и $x = \sum_\iota x_\iota$, где $x_\iota \in M$, то, по предположению, каждый x_ι аннулируется некоторым элементом $\alpha_\iota \neq 0$ кольца A, причем можно считать, что $\alpha_\iota = 1$, если $x_\iota = 0$. Тогда элемент $\alpha = \prod_\iota \alpha_\iota$ отличен от нуля и аннулирует x. Кроме того, равенство $\beta x = 0$ равносильно условию $\beta x_\iota = 0$ для всех ι, и поэтому аннулятор элемента x совпадает с *пересечением* аннуляторов элементов x_ι.

2. *Каноническое разложение модуля кручения над кольцом главных идеалов*

Пусть M — модуль над коммутативным кольцом A. Если α, β — элементы кольца A и α делит β, то, очевидно, $M(\alpha) \subset M(\beta)$. В частности, когда n пробегает множество целых рациональных чисел, подмодули $M(\alpha^n)$ образуют возрастающую последовательность; следовательно, объединение M_α всех $M(\alpha^n)$ является подмодулем, состоящим из тех элементов M, которые аннулируются некоторой степенью элемента α. Ясно, что для всякого подмодуля N модуля M выполняется равенство $N_\alpha = M_\alpha \cap N$.

Определение 2. *Пусть* π *— экстремальный элемент кольца главных идеалов* A. *A-модуль M называется π-модулем, если для всякого* $x \in M$ *существует такое целое число* $n \geqslant 1$, *что* $\pi^n x = 0$ (другими словами, M совпадает со своим подмодулем M_π).

Очевидно, что всякий моногенный модуль вида $A/(\pi^s)$ является π-модулем; подмодуль M_π произвольного A-модуля M также будет π-модулем.

Предложение 3. *Пусть M — модуль кручения над кольцом главных идеалов A и* $\alpha = \varepsilon \prod_{i=1}^{r} \pi_i^{n(i)}$ *— разложение произвольного элемента* $\alpha \neq 0$ *кольца A на экстремальные множители* (§ 1, n° 3, теорема 2). *Тогда подмодуль $N = M(\alpha)$, состоящий из элементов модуля M, аннулируемых элементом α, является прямой суммой подмодулей $M(\pi_i^{n(i)})$ и отображение, которое каждому $x \in M(\alpha)$ ставит в соответствие его компоненту в $M(\pi_i^{n(i)})$, имеет вид $x \to \gamma_i x$ ($\gamma_i \in A$). Кроме того, $M(\pi_i^{n(i)}) = M \cap M_{\pi_i} = N_{\pi_i}$.*

Известно, что $\pi_i^{n(i)}$ независимо с произведением $\alpha_i = \prod_{j \neq i} \pi_j^{n(j)}$ (гл. VI, § 1, n° 12, следствие 3 из предложения 11 (ДЕЛ)); ввиду тождества Безу (§ 1, теорема 1) первая часть доказываемого предложения выводится с помощью индукции по r из следующей леммы:

Лемма 1. *Пусть A — кольцо целостности, α и β — такие элементы кольца A, что $A\alpha + A\beta = A$. Тогда для всякого A-модуля M подмодуль $M(\alpha\beta)$ является прямой суммой подмодулей $M(\alpha)$ и $M(\beta)$ и отображение, ставящее в соответствие каждому $x \in M(\alpha\beta)$ его компоненту в $M(\alpha)$* (соответственно *в $M(\beta)$*), *является гомотетией.*

В самом деле, по предположению, в кольце A существуют такие элементы λ и μ, что $\lambda\alpha + \mu\beta = 1$. Тогда для всякого $x \in M(\alpha\beta)$ выполняется равенство $x = \mu(\beta x) + \lambda(\alpha x)$, причем $\mu\beta x \in M(\alpha)$, $\lambda\alpha x \in M(\beta)$, так как $\alpha\mu\beta x = \mu\alpha\beta x = 0$ и $\beta\lambda\alpha x = \lambda\alpha\beta x = 0$. Следовательно, $M(\alpha, \beta)$ является суммой $M(\alpha)$ и $M(\beta)$; для доказательства того, что эта сумма прямая, достаточно показать, что пересечение $M(\alpha) \cap M(\beta)$ нулевое; но если $x \in M(\alpha) \cap M(\beta)$, то $x = \mu\beta x + \lambda\alpha x = 0$. Наконец, компонента элемента $x \in M(\alpha\beta)$ в $M(\alpha)$ равна $\mu\beta x$, что и доказывает лемму.

Остается доказать, что $M(\pi_i^{n(i)})$ совпадает с множеством элементов N, аннулируемых некоторой степенью π_i. Так как $M(\pi_i^{n(i)}) \subset M_{\pi_i}$ и $M(\alpha)$ — прямая сумма подмодулей $M(\pi_i^{n(i)})$ и $M(\alpha_i)$, то достаточно показать, что если элемент $y \in M(\alpha_i)$ аннулируется степенью π_i^m, то $y = 0$. Но в силу тождества Безу в кольце A найдутся элементы ϱ и σ такие, что $\varrho\pi_i^m + \sigma\alpha_i = 1$; отсюда следует, что $y = \varrho(\pi_i^m y) + \sigma(\alpha_i y)$, а это и заканчивает доказательство.

Теорема 1. *Пусть M — модуль кручения над кольцом главных идеалов A и M_π — его подмодуль, состоящий из элементов, аннулируемых некоторой степенью экстремального элемента $\pi \in A$. Если P — система представителей экстремальных элементов кольца A, то M разлагается в прямую сумму π-модулей M_π, $\pi \in P$.*

Для доказательства используем следующую лемму:

Лемма 2. *Пусть M — модуль кручения над кольцом целостности A. Тогда для всякого конечного множества элементов $(x_i)_{1 \leqslant i \leqslant n}$ этого модуля в кольце A найдется такой элемент $\gamma \neq 0$, что все x_i принадлежат $M(\gamma)$.*

В самом деле, для каждого индекса i в кольце A существует элемент $\alpha_i \neq 0$, который аннулирует x_i; элемент $\gamma = \prod_{i=1}^{n} \alpha_i$ является искомым.

Таким образом, всякий элемент $x \in M$ принадлежит некоторому подмодулю $M(\alpha)$, $\alpha \neq 0$, и, следовательно, по предложению 3, является суммой конечного числа элементов, каждый из которых принадлежит некоторому подмодулю M_π. С другой стороны, если $\sum_{\pi \in P} x_\pi = \sum_{\pi \in P} y_\pi$, где $x_\pi \in M_\pi$, $y_\pi \in M_\pi$ для всех $\pi \in P$, и лишь конечное число элементов x_π и y_π отлично от нуля, то из леммы 2 следует, что в кольце A существует такой элемент $\gamma \neq 0$, что все элементы x_π и y_π принадлежат одному и тому же модулю $M(\gamma)$; отображение на $M(\gamma)$, указанное в предложении 3, показывает, что $x_\pi = y_\pi$ для всякого $\pi \in P$, а это заканчивает доказательство.

Очевидно, что если π и π' — ассоциированные экстремальные элементы, то $M_\pi = M_{\pi'}$; следовательно, подмодули M_π дан-

ного модуля M зависят только от максимальных (главных) идеалов (π) кольца A; эти идеалы называются *π-компонентами* модуля M, а разложение модуля M в прямую сумму модулей M_π называется *каноническим разложением* модуля M в прямую сумму его π-компонент.

Следствие. *Всякий подмодуль N модуля кручения M является прямой суммой подмодулей $N \cap M_\pi$.*

Это следует из того, что $N \cap M_\pi$ является π-компонентой N_π модуля N.

Замечание. Ясно, что аннулятор любого ненулевого элемента π-модуля имеет вид $A\pi^k$ ($k > 0$ — целое число), ибо это главный идеал, содержащий некоторую степень элемента π. Пусть x — элемент модуля M; его аннулятор есть н. о. к. аннуляторов тех x_π, которые отличны от нуля; по предыдущему, этот аннулятор равен произведению аннуляторов элементов $x_\pi \neq 0$ (гл. VI, § 1, предложение 12 (ДЕЛ)).

Определение 3. *Модуль M над произвольным кольцом A называется модулем конечного типа, если он имеет конечную систему образующих.*

Предложение 4. *Если M — модуль кручения конечного типа над кольцом главных идеалов A, то все его π-компоненты, кроме конечного числа, равны нулю и отображение, которое каждому $x \in M$ ставит в соответствие его π-компоненту в π-компоненте M_π модуля M, является гомотетией.*

Это немедленно следует из предложения 3, так как по лемме 2 в кольце A существует такой элемент $\alpha \neq 0$, что $M = M(\alpha)$.

Важный случай применения теоремы 1 и предложения 4 получается, если положить $A = \boldsymbol{Z}$; $\boldsymbol{Z}$-модули представляют собой не что иное, как *абелевы группы* (записываемые аддитивно). Абелева группа называется *группой кручения*, если она является $\boldsymbol{Z}$-модулем кручения, то есть если все ее элементы имеют *конечный порядок*. Пусть P — множество положительных простых чисел. Абелева группа называется *p-группой*, если все ее элементы имеют порядок, равный степени положительного простого числа p. В этой терминологии теорема 1 показывает, что *всякая группа кручения является прямой суммой* p-групп — p-компонент данной группы; для конечной группы множество p-компонент, отличных от единичной подгруппы, конечно.

3. *Применения: I. Каноническое разложение рациональных чисел и рациональных дробей от одного переменного*

Теорема 2. *Пусть A — кольцо главных идеалов, K — его поле дробей и P — система представителей экстремальных элементов кольца A.*

Для произвольного элемента $x \in K$ в P существует такое конечное подмножество H, что x может быть представлен в виде

$$x = a_0 + \sum_{p \in H} a_p p^{-s(p)}, \tag{1}$$

где a_0, a_p — элементы кольца A, a_p не делится на p, и $s(p) > 0$ — целые числа. При этом H и числа $s(p)$ определены однозначно.

Если, кроме того, R_p есть подмножество кольца A, содержащее по одному элементу из каждого класса по mod p *($p \in p$), то всякий $x \in K$ единственным образом может быть записан в виде*

$$x = a + \sum_{p \in P} \sum_{h=1}^{\infty} r_{ph} p^{-h}, \tag{2}$$

где $a \in A$, элементы $r_{ph} \in R_p$ и лишь конечное число их отлично от нуля.

Обозначим через K_A поле K, рассматриваемое как A-модуль. Тогда A есть подмодуль в K_A, порожденный единицей, а модуль K_A/A — фактормодуль по отношению эквивалентности $x' - x \in A$, которое в обозначениях гл. VI, § 1, n° 5 может быть записано в виде $x \equiv x'$ (mod 1); обозначим через f каноническое отображение модуля K_A на $M = K_A/A$.

Модуль M есть *модуль кручения*, так как всякий его элемент имеет вид $f(a/b)$ ($a \in A$, $b \in A$, $b \neq 0$), откуда $bf(a/b) = f(a) = 0$. Следовательно, к нему можно применить теорему 1 n° 2. Пусть M_p ($p \in P$)— подмодуль в M, состоящий из элементов, аннулируемых некоторой степенью элемента p (p-компонента модуля M); тогда $f^{-1}(M_p)$ является подкольцом K_p, состоящим из элементов K вида ap^{-n}, где $a \in A$ и $n \geqslant 0$ — целое число. Так как M есть прямая сумма модулей M_p, то $x \in K$ сравним с некоторым элементом суммы подколец K_p; другими словами, можно написать формулу (1), где $s(p) > 0$ — целые числа, $\{a_p\}$— конечное множество элементов A и a_p не делится на p.

Покажем, что эти условия, наложенные на $s(p)$ и a_p, определяют H и $s(p)$. В самом деле, в этом случае H есть множество элементов $p \in P$ таких, что компонента $f(x)$ в M_p не равна нулю. С другой стороны, если s, $s' > 0$ — целые числа, $s \geqslant s'$, a и a' — элементы A, не делящиеся на p и такие, что $ap^{-s} = a'p^{-s'} \pmod 1$, то $a = a'p^{s-s'} \pmod{p^s}$; если бы выполнялось неравенство $s > s'$, то было бы справедливо сравнение $a \equiv 0 \pmod p$, что противоречит предположению. Это рассуждение показывает, кроме того, что всякое a_p вполне определяется по $\bmod p^{s(p)}$.

Для завершения доказательства заметим сначала, что в каждом классе кольца A по $\bmod p^s$ существует единственный элемент вида $\sum_{h=0}^{s-1} r_p p^h$, где $r_p \in R_p$ для $0 \leqslant h \leqslant s-1$. В самом деле, применим индукцию по s: для $s = 1$ утверждение следует из определения R_p; пусть, по индуктивному предположению, в классе x по $\bmod p^{s-1}$ существует единственный элемент вида $\sum_{h=0}^{s-2} r_p p^h$ ($r_p \in R_p$); тогда $x - \sum_{h=0}^{s-2} r_p p^h$ является кратным ap^{s-1} степени p^{s-1} и существует единственный элемент $r_{s-1} \in R_p$ такой, что $a \equiv r_{s-1} \pmod p$. Отсюда следует, что $x \equiv \sum_{h=0}^{s-1} r_p p^h \pmod{p^s}$. Для получения формулы (2) достаточно применить это рассуждение к каждому a_p в формуле (1). Единственность, ввиду написанного выше, очевидна.

Укажем наиболее важные случаи применения теоремы 2.

I. $A = \boldsymbol{Z}$ — *кольцо целых рациональных чисел, и* $K = \boldsymbol{Q}$. В качестве P берется множество строго положительных простых чисел, а в качестве R_p для любого $p \in R$ берется интервал $[0, p-1]$. Тогда получится каноническое разложение

$$x = a + \sum_{p \in P} \sum_{h=1}^{\infty} e_{ph} p^{-h},$$

где $a \in \boldsymbol{Z}$, $e_{ph} \in \boldsymbol{Z}$, $0 \leqslant e_{ph} \leqslant p-1$.

II. $A = E[X]$ — *кольцо многочленов от одного переменного над полем* E, $K = E(X)$. В качестве R_p берется множество унитарных неприводимых многочленов кольца $E[X]$ (§ 1, n° 4). Из алго-

ритма Евклида следует, что в качестве R_p для любого $p \in R$ (гл. VI, § 1, n° 5) можно взять множество многочленов степени строго меньшей, чем степень P. Тогда получится каноническое разложение рациональной дроби $r(X) \in E(X)$:

$$r(X) = a(X) + \sum_{p \in P} \sum_{h=1}^{\infty} \nu_{ph}(X)\, p(X)^{-h},$$

где $a(X)$— многочлен, $p(X)$— различные унитарные неприводимые многочлены, $\nu_{ph}(X)$ при любых p и h — многочлены, степени которых строго меньше, чем степень $p(X)$. В частности, если E — алгебраически замкнутое поле, то $p(X)$ имеет вид $X - \alpha$, $\alpha \in E$ (гл. V, § 4, предложение 1), а $\nu_{ph}(X)$— константы.

Следовательно, можно сказать, что векторное пространство $E(X)$ над полем K имеет в качестве (линейного) базиса множества одночленов X^n ($n \geqslant 0$ — целое) и рациональных дробей вида $X^m/p(X)^h$, где p пробегает множество P и для всякого p, h пробегает множество целых чисел $\geqslant 1$, а m — множество чисел $0 \leqslant m < \deg p$.

4. *Применения: II. Мультипликативная группа целых чисел по* mod *a*

Пусть $a > 1$ — целое рациональное число и $G(a)$— *мультипликативная* группа обратимых элементов кольца $\boldsymbol{Z}/(a)$. Если $a = \prod_i p_i^{n(i)}$ — разложение числа a на простые множители, то $\boldsymbol{Z}/(a)$ изоморфно произведению колец $\boldsymbol{Z}/(p_i^{n(i)})$ (§ 1, n° 2, предложение 4); по определению произведения колец (гл. I, § 8, n° 10, определение 9), группа $G(a)$ изоморфна произведению групп $G(p_i^{n(i)})$. Таким образом, все сводится к изучению групп $G(p^n)$, где p — простое число. Необратимые элементы кольца $\boldsymbol{Z}/(p^n)$— это элементы единственного максимального идеала $(p)/(p^n)$ этого кольца (гл. I, § 8, теоремы 1 и 5), то есть классы кратных p по mod p^n, и поэтому порядок $\varphi(p^n)$ группы $G(p^n)$ равен $p^n - p^{n-1} = p^{n-1}(p-1)$.

Мы воспользуемся в дальнейшем следующей леммой:

Лемма 3. *Для всякого целого числа $k \geqslant 0$ выполняются сравнения:*

$$(1+p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}} \tag{3}$$

для любого простого числа $p > 2$;

$$5^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}}. \tag{4}$$

Для $k = 0$ сравнение (3) очевидно; для $k = 1$ оно следует из того, что биномиальные коэффициенты $\binom{p}{r}(1 < r < p)$ — целые числа, кратные p (гл. VI, § 1, n° 2). При $k \geqslant 1$ проведем индукцию по k: для любого целого числа b выполняются сравнения

$$(1 + p^{k+1} + bp^{k+2})^p \equiv 1 + p^{k+2} + bp^{k+3} \pmod{p^{2k+2}}.$$

Но $2k + 2 \geqslant k + 3$ и, по предположению индукции (примененному к числу k), $(1 + p)^{p^{k+1}} \equiv 1 + p^{k+2}$. Аналогично, соотношение (4) при $k = 0$ очевидно; при $k \geqslant 0$ применим индукцию по k: для любого целого c

$$(1 + 2^{k+2} + c2^{k+3})^2 \equiv 1 + 2^{k+3} + c2^{k+4} \pmod{2^{k+4}}$$

и $2k + 4 \geqslant k + 4$, откуда, по предположению индукции, $5^{2^{k+1}} \equiv 1 + 2^{k+3} \pmod{2^{k+4}}$. Лемма доказана.

Теперь рассмотрим сначала случай $p > 2$. Тогда сравнение (3) показывает, что для $n > 1$ справедливы соотношения $(1 + p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ и $(1 + p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$; поэтому класс γ по mod p^n, порожденный элементом $1 + p$, имеет в $G(p^n)$ порядок p^{n-1}; но порядок $G(p^n)$ равен $p^{n-1}(p - 1)$, $p - 1$ и p независимы, и p^{n-1} — порядок p-компоненты $G(p^n)$, так что эта p-компонента является циклической группой Γ с образующим γ. По теореме 1 группа $G(p^n)$ является прямым произведением группы Γ и группы Δ порядка $p - 1$. Кроме того, известно, что $G(p)$ — циклическая группа порядка $p - 1$ (гл. V, § 11, n° 3, теорема 2); пусть $r \pmod{p^n}$ — образующий этой группы; для $n > 1$, если $r^k \equiv 1 \pmod{p^n}$, то и $r^k \equiv 1 \pmod{p}$, так что порядок класса ϱ_0 элемента r в группе $G(p)$ делится на $p - 1$. Положив $\varrho_0 = \varrho\lambda$, $\varrho \in \Delta$, $\lambda \in \Gamma$, будем иметь, что порядок элемента ϱ равен $p - 1$, так как порядок λ является степенью числа p (см. замечание к теореме 1). Следовательно, порядок $\varrho\gamma$ в $G(p^n)$ равен $p^{n-1}(p - 1)$ (там же), откуда и следует, что группа $G(p^n)$ — *циклическая*. Так как $\lambda^{p^{n-1}} = 1$ и порядок элемента $\varrho^{p^{n-1}}$ равен $p - 1$ ($p - 1$ взаимно просто с p^{n-1}), то $G(p^n)$ также порождается элементом $\varrho_0^{p^{n-1}}\gamma$.

Пусть теперь $p = 2$ и $n \geqslant 3$. Из соотношения (4) следует, что класс 5 по mod 2^n имеет в $G(2^n)$ порядок 2^{n-2}; все 2^{n-2} чисел вида 5^h $(0 \leqslant h < 2^{n-2})$ попарно несравнимы по mod 2^n. Покажем, что 2^{n-1} чисел вида 5^h и 5^{-h} $(0 \leqslant h < 2^{n-2})$ также попарно несрав-

нимы по mod 2^n; в противоположном случае мы имели бы $5^h + 5^k \equiv 0 \pmod{2^n}$ при $0 \leqslant h < 2^{n-2}$ и $0 \leqslant k < 2^{n-2}$; но если, например, $k \geqslant h$, то отсюда следовало бы сравнение $5^{k-h} \equiv -1 \pmod{2^n}$, то есть $5^{2(k-h)} \equiv 1 \pmod{2^n}$; но тогда, по предыдущему, было бы $k - h = 2^{n-3}$, а из соотношения (4) следует, что $5^{2^{n-3}} \equiv -1 \pmod{2^n}$. Следовательно, $G(2^n)$ является *произведением* циклической группы порядка 2^{n-2}, порожденной классом $5 \pmod{2^n}$, и циклической группы порядка 2, порожденной классом $-1 \pmod{2^n}$.

Так как $G(2)$ и $G(4)$ — циклические группы порядка соответственно 1 и 2, то мы получили следующий результат:

Теорема 3. *Пусть $a > 1$ — целое число и $a = \prod_i p_i^{n(i)}$ — его разложение на простые множители. Тогда мультипликативная группа $G(a)$ кольца $\mathbf{Z}/(a)$ изоморфна произведению групп $G(p_i^{n(i)})$. Если $p > 2$ — простое число, то $G(p^n)$ — циклическая группа порядка $p^{n-1}(p-1)$. Группа $G(1)$ — единичная, $G(4)$ — циклическая порядка 2; наконец, для $n \geqslant 3$ группа $G(2^n)$ — прямое произведение циклической группы порядка 2^{n-2} и циклической группы порядка 2.*

Следствие. *Пусть $a = \prod_i p_i^{n(i)}$ — разложение целого числа $a \geqslant 1$ на простые множители* (i пробегает конечное множество индексов, для которых $n(i) > 0$); *тогда функция Эйлера элемента a* (гл. V, § 11, n° 3) *равна*

$$\varphi(a) = \prod_i \varphi(p_i^{n(i)}) = a \prod_i \left(1 - \frac{1}{p_i}\right). \qquad (5)$$

Упражнения. 1) Пусть x и y — элементы модуля кручения M над кольцом главных идеалов A, $A\alpha$ и $A\beta$ — их аннуляторы, δ — н. о. д. α и β. Показать, что если $A\gamma$ — аннулятор элемента $x + y$, то γ является делителем $\alpha\beta/\delta$ и кратным $\alpha\beta/\delta^2$. Показать также, что если α и β являются *различными* степенями π^μ, π^ν одного и того же экстремального элемента π, то $\gamma = \pi^{\max(\mu, \nu)}$.

2) Пусть π — экстремальный элемент кольца главных идеалов A и M — π-модуль; показать, что для всякого $x \in M$ и всякого $\alpha \in M$, не кратного π, существует единственный элемент $y \in M$ такой, что $x = \alpha y$ (использовать тождество Безу); положим $y = \alpha^{-1}x$. Вывести отсюда, что если $A\pi$ — кольцо главных идеалов, образованное

элементами β/α поля дробей K кольца A, где $\beta \in A$ и $\alpha \in A$ не кратно π (§ 1, упражнение 4), то на M можно единственным образом определить структуру A_π-модуля так, чтобы данная на M структура A-модуля получалась из нее сужением кольца операторов до кольца A.

Полученный таким образом A_π-модуль называется *канонически ассоциированным* с модулем M.

*3) а) Модуль M над кольцом главных идеалов A называется *делимым*, если для всякого $x \in M$ и всякого $\alpha \in A$, отличного от нуля, существует единственный элемент $y \in M$ такой, что $x = \alpha y$. Пусть M — делимый A-модуль, F — произвольный A-модуль, E — его подмодуль и f — линейное отображение модуля E в M; показать, что f может быть продолжено до линейного отображения модуля F в M. (Рассмотреть множество линейных отображений подмодулей F модуля M в M, упорядоченное по продолжению, и применить теорему Цорна.) Вывести отсюда, что всякий делимый подмодуль A-модуля F обладает в F дополнением.

б) Пусть M — делимый модуль над кольцом главных идеалов A, π — экстремальный элемент кольца A и $x_0 \in M$ имеет аннулятор вида $A\pi^n$ (n — целое, $n > 0$). Определим по индукции последовательность (x_s) элементов M: $x_s = \pi x_{s+1}$ для любого целого $s > 0$. Показать, что подмодуль, порожденный в M последовательностью (x_s), изоморфен π-компоненте A_π модуля $U = K_A/A$ (см. n° 3).

в) Модуль называется *неразложимым*, если он не является прямой суммой двух подмодулей, отличных от него и от $\{0\}$. Показать, что U_π — делимый модуль и всякий его подмодуль, отличный от U_π и от $\{0\}$, моногенный и порождается классом по mod A некоторой степени элемента π; вывести отсюда, что модуль U_π неразложим.

г) Показать, что всякий неразложимый делимый A-модуль изоморфен K_A (n° 3) или одному из модулей U_π (использовать а) и б)).

д) Показать, что всякий делимый A-модуль является прямой суммой некоторого семейства своих неразложимых подмодулей (применить теорему Цорна к семействам неразложимых делимых подмодулей модуля M, сумма которых прямая).

*4) Семейство (x_ι) элементов модуля M над кольцом главных идеалов A называется *псевдосвободным*, если из любого соотношения вида $\sum \alpha_\iota x_\iota = \beta y$ ($y \in M$, $\alpha_\iota \in A$, $\beta \in A$) следует, что существуют такие элементы $\alpha'_\iota \in A$, что $\alpha_\iota x_\iota = \beta \alpha'_\iota x_\iota$ для всякого индекса ι. В этом случае из $\iota = \varkappa$ следует, что $x_\iota \neq x_\varkappa$; множество элементов псевдосвободного семейства называется псевдосвободной частью модуля M.

а) Пусть π — экстремальный элемент кольца A; показать, что в A-модуле с аннулятором $A\pi^n$ всякий элемент, аннулятор которого совпадает с $A\pi^n$, псевдосвободен (использовать теорему Безу).

б) Пусть (x_ι) — псевдосвободное семейство A-модуля M, и N — порожденный им подмодуль. Показать, что для всякого $\dot{x} \in M/N$

существует элемент $x \in \dot{x}$, аннулятор которого совпадает с аннулятором класса $\dot{x}$ в M/N. Показать также, что если, кроме того, класс $\dot{x}$ псевдосвободен в M/N, то семейство, составленное из x_ι и x, псевдосвободно в M/N.

в) Вывести из а) и б), что если аннулятор A-модуля M отличен от нуля, то M является прямой суммой моногенных модулей (доказательство свести к случаю π-модуля и применить теорему Цорна к псевдосвободным семействам элементов модуля M).

5) Пусть M — модуль кручения конечного типа над кольцом главных идеалов A. Показать, что M обладает рядом Жордана — Гельдера (воспользоваться упражнением 4в)). Вывести отсюда, что всякое непустое множество его подмодулей обладает максимальным и минимальным элементами (гл. I, § 6, следствие теоремы 8).

*6) Пусть M — модуль кручения над кольцом главных идеалов A, причем все подмодули M, кроме самого M, являются модулями конечного типа. Показать, что существует экстремальный элемент $\pi \in A$ такой, что модуль M изоморфен π-компоненте U_π модуля $U = K_A/A$ (упражнение 3в)). (Показать сначала, что модуль M не может иметь более одной ненулевой π-компоненты и, следовательно, является π-модулем для некоторого экстремального элемента $\pi \in A$. С помощью упражнения 4 показать, что все модули $\pi^n M$ отличны от нуля; из упражнения 5 вывести, что соотношение $\pi M \neq M$ влечет $\pi^n M = \pi^{n+1} M$ для некоторого $n \geqslant 1$; с помощью упражнения 3 показать, что это невозможно).

*7) Пусть M — модуль над кольцом главных идеалов A. Подмодуль N модуля M называется *чистым*, если для всякого элемента $\alpha \in A$ выполняется равенство $N \cap (\alpha M) = \alpha N$.

а) Подмодуль N чист тогда и только тогда, когда для любого $\alpha \in A$ и любого $\dot{x} \in M/N$, имеющего аннулятор $A\alpha$, существует элемент $x \in \dot{x}$ с аннулятором $A\alpha$.

б) Показать, что подмодуль кручения модуля M чистый. Для того чтобы семейство (x_ι) элементов модуля M было псевдосвободным (упражнение 4), необходимо и достаточно, чтобы сумма подмодулей Ax_ι была прямой и являлась чистым подмодулем. Показать, что если P и Q — подмодули модуля M такие, что $P \cap Q$, и $P + Q$ — чистые подмодули, то P и Q — также чистые подмодули.

в) Показать, что всякий подмодуль N модуля M, обладающий дополнением в M, чистый. Показать, что, обратно, если N — чистый подмодуль модуля M и M/N — прямая сумма моногенных подмодулей, то N обладает дополнением в M (использовать а)).

г) Пусть N — чистый подмодуль модуля M, и $A\alpha \neq (0)$ — его аннулятор. Показать, что сужение на N канонического гомоморфизма f модуля M на $M/\alpha M$ является изоморфизмом N на $f(N)$. Показать,

что $f(N)$ является чистым подмодулем в $M/\alpha M$ (рассмотреть π-компоненты фактормодуля $M/\alpha M$ и, применив упражнение 2, свести доказательство к случаю, когда $f(y) = \delta f(z)$, где $y \in N$, $z \in M$ и δ делится на α. Вывести отсюда (используя в) и упражнение 4в)), что подмодуль $f(N)$ и подмодуль N обладают дополнениями в $M/\alpha M$ и M соответственно. В частности, если подмодуль кручения модуля M обладает ненулевым аннулятором (что бывает в случае, когда модуль M конечного типа), то он обладает дополнением в M (см. § 4, следствие 1 теоремы 2).

д) Пусть p — простое число; обозначим через N $\boldsymbol{Z}$-модуль, являющийся прямой суммой моногенных модулей $\boldsymbol{Z}/(p^n)$ $(n \geqslant 1)$, и через e_n — элемент модуля N, у которого координата с номером n равна классу 1 (mod p^n), а все остальные координаты равны нулю. Пусть M — подмодуль $\boldsymbol{Z}$-модуля $N \times Q$, порожденный элементами (e_n, p^{-n}). Показать, что подмодуль кручения P модуля M не обладает в M дополнением (установить, что всякий элемент модуля M/P делится на p^n при любом n, но ни один элемент M, не кратный (0, 1), не обладает этим свойством).

8) Пусть A — кольцо главных идеалов, π — его экстремальный элемент и M — π-модуль. Говорят, что элемент $x \in M$ имеет *высоту* n, если $x \in \pi^n M$ и $x \in \pi^{n+1}M$. Элемент x называется элементом *бесконечной высоты*, если $x \in \pi^n M$ для всех $n \geqslant 1$.

а) Показать, что модуль M делим тогда и только тогда, когда все его элементы бесконечной высоты (упражнение 3).

б) Пусть $x \in M$ — элемент высоты n и $\pi x = 0$; показать, что если $x = \pi^n y$, то моногенный подмодуль Ay модуля M обладает в M дополнением (заметить, что Ay — чистый подмодуль, и применить упражнение 7г)).

в) Показать, что всякий неделимый π-модуль M содержит по крайней мере один моногенный подмодуль, обладающий дополнением. (Пусть $x \in M$ — элемент конечной высоты и существуют целые числа m такие, что элементы $\pi^m x \neq 0$ и имеют бесконечную высоту; пусть s — наименьшее из этих чисел; записать равенство $\pi^s x = \pi y$, где высота y строго больше высоты $\pi^{s-1}x$, и к элементу y — $\pi^{s-1}x$ применить б).)

Вывести отсюда, что всякий неразложимый π-модуль моногенен и изоморфен модулю U_π (упражнение 3).

9) а) Пусть M — π-модуль и M_0 — его подмодуль, состоящий из элементов бесконечной высоты. Показать, что π-модуль M/M_0 не содержит элементов бесконечной высоты.

б) Пусть p — простое число и E — p-группа, прямая сумма групп $E_n = \boldsymbol{Z}/(p^n)$ $(n \geqslant 1)$; обозначим через $e_n \in E_n$ класс 1 (mod p^n). Пусть H — подмодуль E, порожденный элементами $e_1 - p^{n-1}e_n$, $n \geqslant 2$, и $M = E/H$. Показать, что в M подмодуль M_0, состоящий из элементов бесконечной высоты, есть $(E_1 + H)/H$ и изоморфен E_1; поэтому ни один элемент из M_0 не имеет бесконечной высоты в M_0.

*10) а) Пусть M — π-модуль без элементов бесконечной высоты и N — его чистый подмодуль, порожденный максимальным псевдо-

свободным семейством элементов модуля M (упражнения 4 и 7б)). Показать, что M/N — делимый модуль (рассуждать от противного, применяя упражнения 8в), 7в), 7б) и в заключение упражнение 4в)).

°б) Рассмотрим на модуле M метризуемую топологию $\mathscr{T}$; взяв в качестве фундаментальной системы окрестностей нуля подмодули $\pi^n M$, $n \geqslant 0$ (Общ. топол., гл. III, § 1, n° 2). Для того чтобы фактормодуль M/p был делимым, необходимо и достаточно, чтобы подмодуль P был всюду плотен в M в топологии $\mathscr{T}$.

в) P_1 и P_2 — всюду плотные в M в топологии $\mathscr{T}$ чистые подмодули, являющиеся прямыми суммами моногенных подмодулей. Показать, что P_1 и P_2 изоморфны (заметить, что для всякого n фактормодуль $P_1/\pi^n P_1$ изоморфен $M/\pi^n M$).

г) Пусть $\hat{M}$ — пополнение M в топологии $\mathscr{T}$ (Общ. топол., гл. III, § 2, n° 7). Показать, что для всякого $\alpha \in A$ отображение $x \to \alpha x$ является (топологическим) гомоморфизмом $\hat{M}$ на $\alpha\hat{M}$, что для любого целого числа n подмодуль $\pi^n\hat{M}$ открыт и замкнут и является замыканием множества $\pi^n M$, а фактормодули $\hat{M}/\pi^n\hat{M}$ и $M/\pi^n M$ изоморфны.

д) Пусть $\overline{M}$ — модуль кручения модуля $\hat{M}$; показать, что $\overline{M}$ — π-модуль, $\overline{\overline{M}} = \overline{M}$, и M — чистый подмодуль в $\overline{M}$.

е) Пусть π-модуль M является прямой суммой множества $(E\alpha)$ моногенных подмодулей. Топология $\mathscr{T}$ не дискретна тогда и только тогда, когда аннулятор модуля M равен нулю. Обозначим в этом случае через E произведение модулей ΠE_α, и пусть F — подмодуль E, состоящий из элементов, у которых не более чем *счетное* множество координат отлично от нуля; показать, что модуль M можно отождествить (как топологический модуль) с подмодулем F, образованным элементами (x_α) такими, что для любого целого n существует лишь *конечное* число индексов α, для которых $x_\alpha \overline{\in} \pi^n E_\alpha$. Показать тогда, что модули M, $\hat{M}$, $\overline{M}$ и F различны. Вывести отсюда, что $\overline{M}$ не является ни прямой суммой моногенных модулей (использовать д)), ни прямой суммой неразложимых модулей (установить, что $\overline{M}$ не содержит элементов бесконечной высоты, и применить упражнение 8в)).

*11) Пусть M — π-модуль, и N — его подмодуль, у которого все ненулевые элементы имеют в M высоту $\leqslant h$.

а) Пусть P — чистый подмодуль M, $P(\pi) \subset N(\pi)$ и $P(\pi) \neq N(\pi)$. Пусть a — элемент из $N(\pi)$, не принадлежащий $P(\pi)$, и x_0 — элемент $a + P(\pi)$, имеющий в M наибольшую высоту k; пусть $x_0 = \pi^k y_0$. Показать, что сумма $P + Ay_0$ прямая и является чистым подмодулем в M.

б) Пусть B есть псевдосвободное подмножество M, причем $P(\pi) \subset N(\pi)$, где P — чистый подмодуль M, порожденный B. Показать, что существует псевдосвободное подмножество $C \supset B$ такое, что

$Q(\pi) = N(\pi)$, где Q — чистый подмодуль, порожденный C (воспользоваться упражнением а), применить теорему Цорна).

*12) а) π-модуль M является прямой суммой моногенных подмодулей тогда и только тогда, когда в нем существует псевдосвободное подмножество H такое, что $M(\pi) = N(\pi)$, где N — чистый подмодуль, порожденный H.

б) Модуль M разлагается в прямую сумму моногенных подмодулей тогда и только тогда, когда он является объединением возрастающей последовательности (P_k) подмодулей, причем высоты ненулевых элементов каждого P_k *ограничены* (для доказательства достаточности использовать а) и упражнение 11б)).

в) Вывести из б), что если модуль M является прямой суммой моногенных подмодулей, то и всякий его подмодуль является прямой суммой моногенных подмодулей.

г) Пусть M — π-модуль со *счетным* множеством (x_k) образующих. Показать, что модуль M является прямой суммой моногенных подмодулей (обозначив через P_k подмодуль, порожденный образующими x_i, $i \leqslant k$, применить к возрастающей последовательности P_k упражнение б) воспользоваться упражнением 5, примененным к убывающей последовательности $P_k \cap \pi^j M$ (при фиксированном k)).

*13) Пусть π — экстремальный элемент кольца главных идеалов A, M — π-модуль над кольцом A. Пусть I — множество ординальных чисел α (Теор. мн., гл. III) таких, что мощность множества ординальных чисел $\leqslant\alpha$ не превосходит мощности M. Для каждого $\alpha \in I$ следующим образом определим подмодуль $M^{(\alpha)}$ модуля M: $M^0 = M$; если α имеет предшествующий $\alpha - 1$, то $M^{(\alpha)} = \pi M^{(\alpha-1)}$. в противном случае $M^{(\alpha)}$ равно пересечению всех $M^{(\beta)}$ для $\beta < \alpha$.

а) Показать, что существует наименьшее ординальное число $\tau \in I$, *последнее* для M, такое, что $M^{(\tau+1)} = M^{(\tau)}$. Показать, что $M^{(\tau)}$ обладает дополнением в M и является прямой суммой подмодулей, изоморфных U_π (упражнение 3). π-модуль M называется *приведенным*, если $M^{(\tau)} = \{0\}$.

б) Пусть M — приведенный π-модуль. Показать, что для всякого $x \in M$ существует наибольшее ординальное число $\gamma(x) \leqslant \tau$ такое, что $x \in M^{(\gamma(x))}$ (в частности, $\gamma(0) = \tau$). Обобщая определение из упражнения 8, говорят, что $\gamma(x)$ является *высотой* элемента x в M. Показать, что если $\gamma(x) < \gamma(y)$, то $\gamma(x+y) = \gamma(x)$, и что если $\gamma(x) = \gamma(y)$, то $\gamma(x+y) \geqslant \gamma(x)$. Элемент $x \in M$ называется *собственным* относительно подмодуля $y \in M$, если для всякого $\gamma \in N$ высота $\gamma(x+y)$ не превосходит $\gamma(x)$; показать, что в этом случае $\gamma(x \times y) = \min(\gamma(x), \gamma(y))$ для всех $y \in N$.

в) Пусть α — ординальное число $<\tau$ и $\widetilde{M}(\alpha)$ — подмодуль в $M(\alpha)$, состоящий из элементов x, для которых существует $y \in M^{(\alpha+1)}$, удовлетворяющий условию $\pi x = \pi y$. При фиксированном x и при y,

обладающем этим свойством, элементы $u = x - y$ образуют в подмодуле $M(\pi) \cap M^{(\alpha)}$ класс по mod $M(\pi) \cap M^{(\alpha+1)}$. Пусть φ — канонический гомоморфизм модуля $M(\pi) \cap M^{(\alpha)}$ на его фактормодуль по $M(\pi) \cap M^{(\alpha+1)}$. Показать, что отображение ψ, которое каждому элементу x ставит в соответствие $\varphi(u)$, является гомоморфизмом с ядром $M^{(\alpha+1)}$ и, следовательно, модуль $\widetilde{M}(\alpha)/M^{(\alpha+1)}$ изоморфен $(M(\pi) \cap M^{(\alpha)})/(M(\pi) \cap M^{(\alpha+1)})$.

г) Пусть N — подмодуль M и $x \in \widetilde{M}(\alpha)$ — элемент высоты α; показать, что элемент x — собственный относительно N тогда и только тогда, когда соответствующие ему элементы $u = x - y \in M(\pi) \cap M^{(\alpha)}$ (см. в)) — собственные относительно N. Для существования такого элемента необходимо и достаточно, чтобы образ $N \cap \widetilde{M}(\alpha)$ при гомоморфизме ψ был отличен от $(M(\pi) \cap M^{(\alpha)})/(M(\pi) \cap M^{(\alpha+1)})$.

*14) Пусть M — приведенный π-модуль. В обозначениях упражнения 13 модуль $(M(\pi) \cap M^{(\alpha)})/(M(\pi) \cap M^{(\alpha+1)})$ при любом $\alpha < \tau$ можно рассматривать как векторное пространство над полем $F_\pi = A/A_\pi$; обозначим через $c(\alpha)$ мощность базиса этого пространства (см. гл. II, § 1, упражнение 13); будем называть это число *кратностью* ординального числа α в π-модуле M (см. § 4, п° 7).

а) Показать, что π-модули M и N, являющиеся суммами моногенных подмодулей (откуда следует, что $\tau = \omega$ — наименьшему бесконечному ординальному числу), изоморфны тогда и только тогда, когда кратность любого целого n в них одинакова.

б) Привести пример двух неизоморфных π-модулей без элементов бесконечной высоты, в которых любое целое n имеет одну и ту же кратность (см. упражнение 10е).

в) Пусть M и N — приведенные π-модули со *счетным* множеством образующих. Показать, что если M и N имеют одно и то же последнее число τ и всякое $\alpha < \tau$ имеет в них одну и ту же кратность, то они *изоморфны*.

(Пусть $S \subset M$ и $T \subset N$ — подмодули. Изоморфизм модуля S на модуль T называется *сохраняющим высоту*, если высоты $x \in S$ в M и $h(x)$ в N равны. Задача сводится к следующей: пусть $S \subset M$ и $T \subset N$ — подмодули *конечного* типа, $x \in M \cap CS$, h — изоморфизм S на T, сохраняющий высоту; продолжить h до сохраняющего высоту изоморфизма $\overline{h}$ подмодуля $S + Ax$ на некоторый подмодуль в N, содержащий T. Меняя ролями M и N, можно по индукции определить изоморфизм M на N, сохраняющий высоту. Показать, что можно ограничиться случаем $\pi x \in S$; применяя упражнение 5, выбрать в $(S + Ax) \cap CS$ элемент w_1 наибольшей в M высоты α, затем в $S \cap M^{(\alpha)}$ выбрать элемент w_2 таким образом, чтобы высота $\pi(w_1 + w_2)$ в M была наибольшей; показать, что элемент $w = w_1 + w_2$ — собственный относительно подмодуля S (упражнение 13б)). Пусть $z = h(\pi w) \in T$; показать, что если существует элемент $t \in N$, имеющий в N

высоту α, собственный относительно T и такой, что $\pi t = z$, то искомое продолжение $\overline{h}$ изоморфизма h получается по формуле $\overline{h}(w) = t$. Остается только доказать существование такого элемента t. Если $\gamma(z) = \gamma(\pi w) = \alpha + 1$, то в $N^{(\alpha)} \cap CT$ существуют такие элементы u, что $z = \pi u$, и в качестве t можно взять один из этих элементов. Если же $\gamma(z) = \gamma(\pi w) > \alpha + 1$, то $w \in \widetilde{M}(\alpha)$ (упражнение 13в)), и, заметив, что (в обозначениях этого упражнения) образ $S \cap M^{(\alpha)}$ в $(M(\pi) \cap M^{(\alpha)})/(M(\pi) \cap M^{(\alpha+1)})$ при отображении ψ имеет конечную размерность над полем F_π, докажите существование элемента t с помощью упражнения 13г) *).)

г) Получить из в) новое доказательство упражнения 12г).

§ 3. Свободные модули над кольцом главных идеалов

Пусть A — кольцо целостности и K — его поле дробей. Пусть, далее, M — A-модуль без *кручения* (§ 2, n° 1).

Ранее упоминалось, что канонический гомоморфизм $x \to 1 \otimes x$ модуля M в векторное пространство M_K, полученное из M расширением области операторов A до K, является взаимно однозначным отображением (гл. III, § 2, n° 3, теорема 2). Следовательно, можно представлять себе модуль M вложенным в линейное пространство $M_{(K)}$. Когда в дальнейшем будет употребляться выражение «ранг» (множества, линейного отображения и т. д.), то будет иметься в виду структура векторного пространства, действующая таким образом на M.

Ясно, что любой *свободный* модуль L (гл. II, § 1) над кольцом целостности A не имеет кручения и всякая база L является базой векторного пространства $L_{(K)}$. Но если A не является полем, то всегда существует A-модуль без кручения, не являющийся свободным.

Например, аддитивная группа поля дробей K кольца A, рассматриваемая как A-модуль, не имеет кручения. Однако, если $A \neq K$, этот модуль не является свободным, так как, с одной стороны, любые два элемента в K образуют зависимое множество, с другой стороны, K не является циклическим модулем, ибо в противном случае мы имели бы $K = ab^{-1}A$ ($a \in A$, $b \in A$), откуда $b^{-2} = acb^{-1}$ ($c \in A$), $b^{-1} = ac \in A$ и $K = A$.

Замечание. Для того чтобы модуль без кручения конечного ранга n был свободным, необходимо и достаточно, чтобы он порождался n элементами.

*) Предлагаемый метод доказательства этой теоремы («теоремы Ульма — Цишпина») сообщили нам Дж. Макки и И. Капланский (не опубликовано).

Теорема 1. *Всякий подмодуль M свободного модуля L над кольцом главных идеалов A является свободным A-модулем.*

Пусть $(e_\iota)_{\iota\in I}$ — некоторый базис L, и P_ι — координатные функции этого базиса. Определим на I структуру *вполне упорядоченного* множества (Теор. мн., гл. III) и обозначим через L_ι подмодуль, порожденный элементами e_λ для $\lambda\leqslant\iota$. Положим $M_\iota = M \cap L_\iota$. Координатная функция p_ι отображает модуль M_ι на идеал A_{a_ι} кольца A. Обозначим через a_ι элемент модуля M_ι такой, что $p_\iota(a_\iota) = \alpha_\iota$; если $\alpha_\iota = 0$, то полагаем $a_\iota = 0$. Пусть M'_ι — подмодуль модуля L, порожденный элементами α_λ для $\lambda\leqslant\iota$. Докажем, то $M'_\iota = M_\iota$ для любого ι; отсюда будет следовать, что модуль M порождается множеством элементов $(a_\iota)_{\iota\in I}$. Сделаем индуктивное предположение, что $M'_\lambda = M_\lambda$ для всех $\lambda < \iota$. Тогда для любого элемента $x \in M_\iota$ будем иметь: $p_\iota(x) = \gamma\alpha_\iota$ ($\gamma \in A$), элемент $x - \gamma a_\iota$ является линейной комбинацией конечного числа элементов e_λ, $\lambda < \iota$. Другими словами, $x - \gamma a_\iota$ принадлежит модулю M_λ, $\lambda < \iota$. По индуктивному предположению $x - \gamma a_\iota \in M'_\lambda \subset M_\iota$, то есть $x \in M'_\iota$, откуда $M'_\iota = M_\iota$. Осталось доказать, что множество ненулевых элементов a_ι свободно. Предположим противное, пусть существует линейное соотношение $\sum_\iota \beta_\iota a_\iota = 0$, где не все элементы $\beta_\iota a_\iota$ (среди которых лишь конечное число отличных от нуля) равны нулю. Пусть μ — наибольший из индексов ι таких, что $\beta_\iota a_\iota \neq 0$. Так как $p_\mu(a_\lambda) = 0$ при $\lambda < \mu$, то $p_\mu(\beta_\mu a_\mu) = p_\mu(\sum \beta_\iota a_\iota) = 0$, но $p_\mu(\beta_\mu a_\mu) = \beta_\mu\alpha_\mu$, и так как $a_\mu \neq 0$ по предположению, то $\alpha_\mu \neq 0$, и мы получили, что $\beta_\mu = 0$. Полученное противоречие доказывает теорему.

Предложение 1. *Пусть L — свободный модуль конечного ранга n над кольцом главных идеалов A; тогда любой подмодуль M модуля L является свободным модулем конечного ранга $\leqslant n$.*

Действительно, по теореме 1 модуль M свободен. Ранг модуля M не превосходит n, так как его можно рассматривать как часть векторного пространства L_K, имеющего размерность n над полем дробей K кольца A.

Следствие. *Пусть E — модуль над кольцом главных идеалов A. порожденный n элементами. Тогда любой подмодуль F модуля E*

обладает системой образующих, содержащей не более чем n элементов.

Действительно, существует гомоморфизм f модуля A^n на модуль E (гл. II, § 1, n° 8, предложение 10). Прообраз $f^{-1}(F)$, являющийся свободным модулем ранга $m \leqslant n$, порождается m элементами. Образы этих элементов при отображении f порождают F.

Упражнения. 1) Привести другое доказательство теоремы 1, использующее теорему Цорна (пусть $(e_\iota)_{\iota \in I}$ — некоторый базис модуля L, и J — подмножество множества I; через L_J обозначим подмодуль, порожденный элементами e_ι, индексы которых $\iota \in J$; рассмотреть множество Φ пар $(J, \mathfrak{B}) \in \mathfrak{B}(I) \times \mathfrak{B}(M)$ таких, что $\mathfrak{B}$ является базисом модуля $M \cap L_J$).

2) Распространить теорему 1 на случай, когда L является левым унитарным свободным модулем над некоммутативным кольцом A с единицей без делителей нуля, в котором всякий левый идеал главный.

3) Пусть A — коммутативное кольцо с единицей. Доказать, что если в некотором унитарном свободном A-модуле любой подмодуль свободен, то всякий идеал кольца A главный и A не содержит делителей нуля (то есть A является кольцом главных идеалов).

*4) Пусть M — модуль над кольцом главных идеалов A. Предположим, что M разлагается в прямую сумму циклических подмодулей. Доказать, что любой подмодуль N модуля M разлагается в прямую сумму циклических подмодулей. (Пусть T — подмодуль кручения модуля N. Сначала, пользуясь теоремой 1, доказать, что фактормодуль N/T свободен, и вывести отсюда, что T обладает дополнительным подмодулем в N. Затем доказать, что T разлагается в прямую сумму циклических подмодулей, используя упражнение 12c) к § 2.)

5) Пусть (p_n) — последовательность простых чисел, расположенных по возрастанию. На рациональной плоскости $\boldsymbol{Q}^2$ рассмотрим $\boldsymbol{Z}$-модуль M, порожденный последовательностью (x_n), определяемой следующим образом:

$$x_0 = (1, 0), \qquad x_1 = (0, 1), \qquad x_{n+1} = p_n^{-1}(x_0 + x_n)$$

для $n \geqslant 1$. Доказать, что M имеет ранг 2 и что любой подмодуль ранга 1 в M циклический (установить, что x_0 и x_n образуют базу подмодуля M, порожденного множеством x_i с $i \leqslant n$, и воспользоваться тем, что n/p_n стремится к 0, когда n стремится к $+\infty$ (§ 1, упражнение 20)).

6) Пусть E — модуль без кручения над кольцом главных идеалов A.

а) Доказать, что если F — чистый подмодуль в E, то фактормодуль E/F без кручения, и обратно.

б) Пусть F — подмодуль в E, порожденный псевдосвободным максимальным множеством (§ 2, упражнение 4), F — свободный

и чистый подмодуль модуля E. Доказать, что для любого элемента $\dot{x} \in E/F$ существуют элемент $\alpha \in A$, не являющийся делителем 1, и элемент $\dot{y} \in E/F$ такие, что $\dot{x} = \alpha\dot{y}$, но фактормодуль E/F не обязан быть делимым модулем (см. упражнение 5).

7) Пусть A — кольцо главных идеалов, обладающее единственным максимальным идеалом $A\pi$ (см. § 1, упражнение 4). Пусть E — A-модуль без кручения и M — свободный подмодуль в E такой, что фактормодуль E/M не имеет кручения и является делимым модулем ранга 1. Пусть (e_α) — база модуля M, $\dot{u}$ — ненулевой элемент фактормодуля E/M, u — элемент смежного класса $\dot{u}$; через u_n, $n > 0$, обозначим такой элемент модуля E, что $u \equiv \pi^n u_n \pmod{M}$. Положим $u = \pi^n u_n + \sum_\alpha \lambda_{n\alpha} e_\alpha$.

а) Доказать, что E порождается модулем M и элементами u_n и имеет место включение $\lambda_{n\alpha} - \lambda_{n+1,\,\alpha} \in A\pi^n$ для всех α и всех целых чисел $n > 0$ (см. упражнение 6а)).

°б) В дополнение к предыдущему предположим, что кольцо A полно в топологии $\mathscr{T}$, определенной в A, если в качестве фундаментальной системы окрестностей нуля в A взять идеалы $A\pi^n$ (Общ. топол., гл. III, § 5, n° 4). Положим $\lambda_\alpha = \lim_{n\to\infty} \lambda_{n\alpha}$. Доказать, что если числа μ и μ_α таковы, что элемент $\mu u - \sum_\alpha \mu_\alpha e_\alpha$ принадлежит всякому подмодулю $\pi^n E$, то необходимо выполняется равенство $\mu_\alpha = \lambda_{\alpha\mu}$ при всех α.

°*8) Пусть A — кольцо главных идеалов, обладающее единственным максимальным идеалом $A\pi$ и полное в топологии, определенной в упражнении 7.

а) Доказать, что всякий A-модуль без кручения E конечного ранга, не содержащий делимых подмодулей, свободен (рассмотреть подмодуль M модуля E, порожденный некоторым максимальным псевдосвободным множеством; доказать, используя упражнения 6б) и 7б), что если $M \neq E$, то модуль E содержит делимый подмодуль).

б) Пусть $(a_n)_{n\geqslant 0}$ — каноническая база свободного модуля $E = A^{(N)}$ (прямая сумма бесконечного числа модулей, изоморфных A), и пусть $e_n = a_{n-1} - a_n$ для всех целых чисел $n \geqslant 1$. Доказать, что подмодуль M модуля E, порожденный элементами e_n, чистый, и элементы e_n образуют максимальное псевдосвободное множество, но фактормодуль E/M является делимым и, следовательно, модуль M не обладает дополнительным подмодулем в E.

9) Пусть p — простое число, A — кольцо рациональных чисел вида r/s, где s взаимно просто с p.

Пусть $u = (1, 0)$ и $v = (0, 1)$ — элементы канонического базиса векторного пространства $E = Q^2$ над полем Q. В пространстве E

определим индукцией по n последовательность элементов u_n: $u_0 = u$ и $u_n = pu_{n+1} + v$ для $n \geqslant 0$.

Пусть F — A-модуль, порожденный элементом v и элементами u_n. Доказать, что, хотя модуль F и не является свободным, тем не менее он не содержит делимых подмодулей (см. упражнение 8а)).

*10) Пусть A — кольцо главных идеалов, обладающее бесконечным множеством максимальных идеалов. Доказать, что для любого *бесконечного* множества I A-модуль, являющийся произведением A^I, *не будет свободным*. (Доказательство свести к случаю, когда I — множество целых чисел $\geqslant 1$. Далее рассуждать от противного: надлежащим образом упорядочить последовательность координат, доказать, кроме того, что существует такая последовательность $(a_n)_{n\geqslant 1}$ элементов базиса, что если $a_n = (\alpha_{nm})$, то $\det(\alpha_{ij})_{1\leqslant i\leqslant n,\ 1\leqslant j\leqslant n} \neq 0$ для всех индексов n. Определить вектор $x=(\xi_n)_{n\geqslant 1}$ в A^I таким образом, чтобы для любого индекса n существовали экстремальный элемент π_n и конечная последовательность элементов β_{ni} $(1 \leqslant i \leqslant n-1)$ кольца A такие, что все координаты вектора $x - a_n - \sum_{i=1}^{n-1} \beta_{ni} \cdot a_i$ (в A^I) кратны элементу π_n. Рассуждение вести по индукции. Пусть π_i, ξ_i и β_{ij} определены для $i < n$, $j < i$; в качестве π_n взять элемент, не ассоциированный с элементами π_i при $i < n$ и не делящийся на $\det(\alpha_{ij})$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$; затем определить β_{nj} $(1 \leqslant j \leqslant n-1)$ и ξ_n и применить «Китайскую теорему» (гл. VI, § 1, упражнение 25). Сделать отсюда вывод о существовании линейной комбинации базисных элементов кольца A^I, коэффициенты которой взаимно просты в совокупности и для которой выполняется равенство $y = \pi z$, где $z \in A^I$ и π — экстремальный элемент кольца A.)

§ 4. Модули конечного типа над кольцом главных идеалов

Напомним, что модуль M над кольцом A называется модулем *конечного типа*, если он обладает конечной системой образующих (§ 2, n° 2).

1. Конечные прямые суммы моногенных модулей

Пусть A — коммутативное кольцо с единицей. Напомним (гл. II, § 1, предложение 11), что всякий моногенный унитарный A-модуль изоморфен *фактормодулю* $A/\mathfrak{a}$, где $\mathfrak{a}$ — идеал кольца A. В этом параграфе (n° 3) будет показано, что всякий модуль конечного типа над кольцом главных идеалов разлагается в прямую сумму конечного числа моногенных модулей.

Лемма 1. *Пусть E — унитарный модуль над коммутативным кольцом A, M — подмодуль в E, f — канонический гомоморфизм модуля E на фактормодуль E/M, $\overline{f}$ — гомоморфизм внешней алгебры $\bigwedge E$ на внешнюю алгебру $\bigwedge (E/M)$, полученный из f каноническим продолжением* (гл. III, § 5, n° 9). *Тогда ядро $\overline{f}$ является двусторонним идеалом $\mathfrak{a}$ алгебры $\bigwedge E$, порожденным M.*

Так как $\overline{f}(M) = \{0\}$, то $\overline{f}(\mathfrak{a}) = 0$ и, следовательно, $\mathfrak{a}$ содержится в ядре $\overline{f}$. Переходя к фактормодулю, получаем, что $\overline{f}$ является гомоморфизмом g факторалгебры $(\bigwedge E)/\mathfrak{a}$ на модуль $\bigwedge (E/M)$. Лемма будет доказана, если мы покажем, что g является на самом деле изоморфизмом. Для доказательства определим отображение h алгебры $\bigwedge (E/M)$ на факторалгебру $(\bigwedge E)/\mathfrak{a}$ такое, что композиция $h \circ g$ будет тождественным автоморфизмом факторалгебры $(\bigwedge E)/\mathfrak{a}$.

Заметим, что всякий элемент идеала $\mathfrak{a}$ представим в виде суммы элементов вида $u \wedge x \wedge v$, где $u \in \bigwedge E$, $v \in \bigwedge E$ и $x \in M$. Разлагая элементы u и v в сумму однородных элементов, получим, что идеал $\mathfrak{a}$ разложим в прямую сумму однородных компонент $\mathfrak{a}_n = (\bigwedge^n E) \cap \mathfrak{a}$. Следовательно, $(\bigwedge E)/\mathfrak{a}$ является прямой суммой однородных компонент $(\bigwedge^n E)/\mathfrak{a}_n$ (гл. I, § 6, предложение 5). Пусть g_n — сужение отображения g на $(\bigwedge^n E)/\mathfrak{a}_n$. Теперь достаточно для любого n определить отображение h_n модуля $\bigwedge^n (E/M)$ на модуль $(\bigwedge^n E)/\mathfrak{a}_n$ так, чтобы композиция $h_n \circ g_n$ была тождественным отображением модуля $(\bigwedge^n E)/\mathfrak{a}_n$ на себя. Для этого рассмотрим полилинейное отображение k_n модуля E^n в модуль $(\bigwedge^n E)/\mathfrak{a}_n$, которое смежному классу элемента $(x_1, \ldots, x_n)$ ставит в соответствие смежный класс элемента $x_1 \wedge \ldots \wedge x_n$ в $(\bigwedge^n E)/\mathfrak{a}_n$. Так как $k_n(x_1, \ldots, x_n)$ равно нулю всякий раз, когда один из x_i принадлежит M, то k_n индуцирует полилинейное отображение $\overline{k}_n$ модуля $(E/M)^n$ в $(\bigwedge^n E)/\mathfrak{a}_n$. По определению, отображение k_n является кососимметрическим, следовательно, таковым же является и отображение $\overline{k}_n$ и тем самым (гл. III, § 5, схолия к определению 5) определено линейное отображе-

ние h_n модуля $\bigwedge^n (E/M)$ в модуль $(\bigwedge^n E)/\mathfrak{a}_n$. Так как отображение g_n ставит в соответствие смежному классу элемента $x_1 \wedge \ldots \wedge x_n$ в $(\bigwedge^n E)/\mathfrak{a}_n$ элемент $f(x_1) \wedge \ldots \wedge f(x_n)$ в $\bigwedge^n (E/M)$, то ясно, что композиция $h_n \circ g_n$ является тождественным автоморфизмом модуля $(\bigwedge^n E)/\mathfrak{a}_n$.

Предложение 1. *Пусть E — унитарный модуль над коммутативным кольцом A; предположим, что E есть прямая сумма n моногенных модулей $A/\mathfrak{a}_k$ $(1 \leqslant k \leqslant n)$, где $\mathfrak{a}_k$ — идеалы кольца A. Тогда для любого целого числа $p > 0$ модуль $\bigwedge^p E$ является прямой суммой модулей $A/\mathfrak{a}_H$, где через $\mathfrak{a}_H$ для любого подмножества $H = \{k_1, \ldots, k_p\}$ из p элементов отрезка натурального ряда $[1, n]$ обозначен идеал $\sum_{j=1}^{p} \mathfrak{a}_{k_j}$ кольца A, порожденный объединением идеалов $\mathfrak{a}_{k_j}$ $(1 \leqslant j \leqslant p)$.*

Пусть x_k — образующий элемент модуля $A/\mathfrak{a}_k$, являющийся каноническим образом единицы кольца A. Пусть (l_k) $(1 \leqslant k \leqslant n)$ — канонический базис модуля A^n, f — гомоморфизм модуля A^n на модуль E, определяемый равенствами $f(e_k) = x_k$ $(1 \leqslant k \leqslant n)$, и $\overline{f}$ — гомоморфизм алгебры $\bigwedge(A^n)$ на алгебру $\bigwedge E$, полученный каноническим продолжением f. Для любого целого p модуль $\bigwedge^p (A^n)$ является свободным модулем с базисом $(e_H) = (e_{k_1} \wedge \ldots \wedge e_{k_p})$, где $H = \{k_1, \ldots, k_p\}$ пробегает всевозможные p-элементные подмножества отрезка натурального ряда $[1, n]$ (гл. III, § 5, n° 9).

Так как ядро отображения f является суммой $\sum_{k=1}^{n} \mathfrak{a}_k e_k$, то ядро отображения $\overline{f}$ порождается элементами суммы $\sum_{k=1}^{n} \mathfrak{a}_k e_k$ в силу леммы 1. Это ядро состоит из суммы элементов вида $u \wedge x \wedge v$, где $u \in \bigwedge(A^n)$, $v \in \bigwedge(A^n)$ и $x = \sum_{k=1}^{n} \alpha_k e_k$, $\alpha_k \in \mathfrak{a}_k$. Если записать u и v как линейные комбинации элементов канонического базиса A-модуля $\bigwedge(A^n)$, то станет очевидным, что ядро отображения $\overline{f}$ состоит из сумм элементов вида $\alpha \cdot e_{k_1} \wedge \ldots \wedge e_{k_q}$,

где α принадлежит по крайней мере одному из идеалов $\mathfrak{a}_{k_j}$ $(1 \leqslant j \leqslant q)$. Другими словами, ядро отображения $\overline{f}$ есть прямая сумма модулей $\mathfrak{a}_H e_H$, где H пробегает всевозможные подмножества отрезка натурального ряда $[1, n]$. Отсюда легко получается нужный результат.

Замечание. Можно доказать, что внешняя алгебра $\bigwedge(\sum_i E_i)$ конечной прямой суммы $\sum_i E_i$ A-модулей изоморфна, как модуль, тензорному произведению $\bigotimes_i (\bigwedge E_i)$ (см. гл. III, § 5, упражнение 7). Применим это соображение для доказательства предложения 1: имеем $E = \sum_i Ax_i$, так что внешняя алгебра $\bigwedge E$ изоморфна (как модуль) тензорному произведению $\bigotimes_i (\bigwedge (Ax_i))$. Далее, внешняя алгебра $\bigwedge (Ax_i)$ является прямой суммой $A + Ax_i$, так как внешнее произведение любых двух элементов из Ax_i равно нулю. Следовательно, внешняя алгебра $\bigwedge E$ есть прямая сумма модулей, каждый из которых является прямой суммой некоторого числа Ax_i (см. гл. III, § 1, предложение 7). Так как $(Ax_{k_1}) \otimes \ldots \otimes (Ax_{k_p})$ — моногенный A-модуль, аннулятор которого есть сумма аннуляторов $\mathfrak{a}_{k_j}$ модулей Ax_{k_j} (гл. III, § 1, п. 3, следствие предложения 6), то мы получаем второе доказательство предложения 1 (не использующее лемму 1).

Теперь можно заметить, что, в обозначениях предложения 1, если идеалы $\mathfrak{a}_k$ образуют возрастающую последовательность, то они однозначно определяются самим модулем E. Более точно:

Предложение 2. *Пусть A — коммутативное кольцо и E — A-модуль, являющийся прямой суммой n моногенных модулей $A/\mathfrak{a}_k$, и идеалы $\mathfrak{a}_k$ таковы, что $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_n \neq A$. Тогда для $1 \leqslant p \leqslant n$ идеал $\mathfrak{a}_p$ есть аннулятор модуля $\bigwedge^p E$; модуль $\bigwedge^p E$ ненулевой при $1 \leqslant p \leqslant n$ и $\bigwedge^m E = \{0\}$ при $m > n$.*

Действительно, в обозначениях предложения 1 имеем $\mathfrak{a}_H = \mathfrak{a}_{s(H)}$, где $s(H)$ — наибольший элемент множества H. Так как $s(H) \geqslant p$ для любого множества H из p элементов и $s(H) = p$ для $H = \{1, 2, \ldots, p\}$, то идеал $\mathfrak{a}_p$ есть пересечение идеалов $\mathfrak{a}_H$, где H пробегает совокупность p-элементных подмножеств отрезка натурального ряда $[1, n]$. Следовательно, идеал $\mathfrak{a}_p$, в силу предложения 1, есть аннулятор модуля $\bigwedge^p E$.

Следствие. *Пусть, в обозначениях предложения 2, π-модуль E изоморфен также прямой сумме m моногенных модулей $A/\mathfrak{a}'_j$, причем $\mathfrak{a}'_1 \subset \ldots \subset \mathfrak{a}'_m \neq A$. Тогда $m = n$ и $\mathfrak{a}_k = \mathfrak{a}'_k$ для $1 \leqslant k \leqslant n$* («единственность идеалов $\mathfrak{a}_k$»).

2. *Инвариантные факторы подмодуля*

Всякий модуль конечного типа над кольцом главных идеалов A можно рассматривать как фактормодуль некоторого свободного модуля по одному из его подмодулей, который, будучи свободным, также является модулем конечного типа (гл. II, § 1, п° 8, предложение 10 и гл. VII, § 3, предложение 1). Сейчас мы изучим в более общем виде взаимосвязь между (произвольным) свободным A-модулем и некоторым его подмодулем конечного типа:

Теорема 1. *Пусть L — свободный модуль над кольцом главных идеалов A и M — его подмодуль конечного ранга. Тогда существуют базис B модуля L, n элементов e_i базиса B и n ненулевых элементов α_i кольца A $(1 \leqslant i \leqslant n)$ такие, что*: а) *элементы $\alpha_i e_i$ образуют базис модуля M*; б) *α_i делит α_{i+1} $(1 \leqslant i \leqslant n-1)$.*

Более того, этими условиями модуль M' с базисом (e_i) и главные идеалы $A\alpha_i$ определяются однозначно; фактормодуль M'/M является модулем кручения модуля L/M и изоморфен прямой сумме A-модулей $A/A\alpha_i$; наконец, L/M является прямой суммой M'/M и некоторого свободного модуля, изоморфного L/M.

1) *Существование элементов e_0 и α_i.*

При $M = \{0\}$ теорема тривиальна. Будем, следовательно, предполагать, что $M \neq \{0\}$, и докажем прежде всего существование элементов $e_1 \in L$ и $\alpha_1 e_1 \in M$ $(\alpha_1 \in M)$ таких, что подмодули Ae_1 и $A\alpha_1 e_1$ обладают дополнениями в L и M соответственно.

Для любой линейной формы f на L образ $f(M)$ есть идеал кольца A, который, по предположению, является главным. Среди этих идеалов $f(M)$ существует максимальный (§ 1, лемма к теореме 2), пусть это будет $A\alpha_1$, соответствующий линейной форме f_1. Пусть u — такой элемент M_1, что $\alpha_1 = f(u)$. Так как $M \neq \{0\}$, то $\alpha_1 \neq 0$. Докажем, что если g — некоторая линейная форма на L, то $g(u) \in A\alpha_1$. В самом деле, пусть $\beta = g(u)$. Идеал

$A\alpha_1 + A\beta$ есть главный идеал $A\gamma$, поэтому в кольце A существуют такие элементы λ и μ, что $\gamma = \lambda\alpha_1 + \mu\beta$. Обозначим через f линейную форму $\lambda f_1 + \mu g$; тогда $\gamma = f(u) \in f(M)$, откуда $f(M) \supset A\gamma \supset A\alpha_1$. По определению $f(M)$ получаем, что $A\gamma = A\alpha_1$, следовательно, $\beta \in A\alpha_1$.

В частности, все координаты элемента u относительно некоторого базиса (x_i) модуля L принадлежат идеалу $A\alpha_1$. Отсюда заключаем, что существует элемент $e_1 \in L$, для которого $u = \alpha_1 e_1$. Тогда $f_1(e_1) = 1$. При этих условиях модуль L есть прямая сумма Ae_1 и $L_1 = f^{-1}(0)$. Действительно, пересечение этих подмодулей равно $\{0\}$, ибо из условия $f_1(\lambda e_1) = 0$ находим $\lambda = \lambda \cdot 1 = \lambda f_1(e_1) = 0$. С другой стороны, любой элемент $x \in L$ есть сумма элемента $f_1(x)\, e_1$ и элемента $y = x - f_1(x)\, e_1$, для которого $f_1(y) = 0$. В свою очередь, модуль M есть прямая сумма подмодулей $A\alpha_1 e_1$ и $M_1 = M \cap f_1^{-1}(0)$. В самом деле, мы уже выяснили, что пересечение этих подмодулей равно $\{0\}$; для любого $x \in M$ образ $f_1(x)$ записывается в виде $\gamma\alpha_1$ ($\gamma \in A$), и элемент x есть сумма элемента $\gamma\alpha_1 e_1$ и элемента $y = x - \gamma\alpha_1 e_1$ такого, что $f_1(y) = 0$. Кроме того, модуль L_1 свободен, как подмодуль свободного модуля (§ 3, теорема 1). Пусть g — некоторая линейная форма на L, тогда $g(M_1) \subset A\alpha_1$. Действительно, в противном случае, так как L есть прямая сумма подмодулей L_1 и Ae_1, на L можно определить линейную форму g', совпадающую с g на L_1 и с f_1 на Ae_1, и $g'(M) = g(M_1) + A\alpha_1 \neq A\alpha_1$, что противоречит максимальности идеала $A\alpha_1$.

Теперь доказательство можно вести индукцией по рангу n модуля M. Так как L_1 — свободный модуль и M_1 имеет ранг $n - 1$, то существуют базис B_1 модуля L_1, $n - 1$ элементов $e_2, \ldots, e_n$ базиса B_1 и ненулевые элементы $\alpha_2, \ldots, \alpha_n$ кольца A такие, что $(\alpha_2 e_2, \ldots, \alpha_n e_n)$ есть базис модуля M_1 и α_i делит α_{i+1} при $2 \leqslant i \leqslant n - 1$. Если L' — подмодуль L, порожденный элементами B_1, отличными от $e_2, \ldots, e_n$, то L есть прямая сумма модуля L' и модуля M', порожденного элементами $e_1, \ldots, e_n$; $(e_1, \ldots, e_n)$ — базис M' и $(\alpha_1 e_1, \ldots, \alpha_n e_n)$ — базис модуля M. Осталось доказать, что α_1 делит α_2. Действительно, $A\alpha_2$ совпадает с $g(M_1)$, где g — линейная форма на L, определяемая равенствами $g(e_2) = 1$, $g(e_i) = 0$ при $i \neq 2$, $g(L') = 0$. В силу доказанного выше $g(M) \subset A\alpha_1$.

2) *Свойства единственности.*

Так как элементы α_i отличны от нуля, то M' совпадает с множеством элементов $x \in L$, для которых существует такой элемент $\beta \neq 0$ кольца A, что $\beta x \in M$.

Другими словами, фактормодуль M'/M является подмодулем кручения для модуля L/M. Это доказывает однозначную определенность модуля M'.

Из свойств факторгрупп (гл. I, § 6, предложение 5), используя базис (e_i), легко установить, что фактормодуль M'/M изоморфен прямой сумме n моногенных модулей $A/A\alpha_i$. Пусть r — число идеалов $A\alpha_i$, отличных от A; таким образом, первые $n-r$ идеалов $A\alpha_i$ совпадают с A, последние r отличны от A. Тогда фактормодуль M'/M изоморфен прямой сумме модулей $A/A\alpha_n, \ldots$ $\ldots, A/A\alpha_{n-r+1}$, где $A\alpha_n \subset A\alpha_{n-r+1} \subset \ldots \subset A\alpha_{n-r+1} = A$. Мы находимся в условиях, когда можно применить следствие к предложению 2 (n° 1): целое число r и идеалы $A\alpha_i$ $(n-r+1 \leqslant i \leqslant n)$ однозначно определяются фактормодулем M'/M. Идеалы $A\alpha_i$, совпадающие с A $(1 \leqslant i \leqslant n-r)$, однозначно определяются, следовательно, модулями L и M, так как n есть ранг M. Так как L является прямой суммой модулей M' и L', то фактормодуль L/M есть сумма M'/M и $(L'+M)/M$; эта сумма прямая, ибо $M' \cap (L'+M) = M$. С другой стороны, фактормодуль $(L'+M)/M$ изоморфен $L'/(M \cap L')$ (гл. I, § 6, n° 13, теорема 6), то есть L', а это доказывает, что последний модуль свободен и изоморфен фактормодулю L/M'.

Следствие. *Для того чтобы подмодуль конечного ранга M свободного модуля L над кольцом главных идеалов A обладал дополнительным подмодулем, необходимо и достаточно, чтобы фактормодуль L/M был модулем без кручения. В частности, для того чтобы моногенный подмодуль Ax $(x \neq 0)$ модуля L обладал дополнительным подмодулем, необходимо и достаточно, чтобы из равенства $x = \alpha y$ $(\alpha \in A)$ следовала обратимость элемента α в кольце A.*

В обозначениях теоремы 1, если L/M есть модуль без кручения, то $M = M'$, и M' обладает дополнительным подмодулем L' в L. Обратно, если M обладает дополнительным подмодулем L' в L, то фактормодуль L/M изоморфен L', и L является свободным модулем (§ 3, теорема 1), то есть и подавно модулем без кручения.

С другой стороны, тот факт, что фактормодуль L/Ax является модулем без кручения, можно выразить еще и так: из включения $\beta y \in Ax$ ($\beta \neq 0$) следует, что $y \in Ax$. Пусть это условие выполняется; тогда из равенства $x = \alpha y$ ($\alpha \in A$) следует существование элемента $\lambda \in A$ такого, что $y = \lambda x$, откуда $x = \alpha\lambda x$, и так как x — свободный элемент, то $\alpha\lambda = 1$. Обратно, если из равенства $x = \alpha y$ следует обратимость элемента α, то, применяя теорему 1 к подмодулю Ax, мы получим, что Ax обладает дополнительным подмодулем в L.

Замечания. 1) Ненулевой элемент x свободного модуля L, обладающий свойством, что из равенства $x = \alpha y$ ($y \in L$, $\alpha \in A$) следует обратимость элемента α, называется *неделимым*.

2) Можно указать пример такого подмодуля M *бесконечного* ранга в свободном модуле L, что фактормодуль L/M является модулем без кручения, но M не обладает дополнительным подмодулем в L (§ 3, упражнение 8б)).

Определение 1. *В предположениях и обозначениях теоремы* 1 *идеалы* $A\alpha_i$ *кольца* A *называются инвариантными факторами подмодуля* M *относительно модуля* L.

В случае, когда A есть кольцо многочленов $K[x]$ от одного переменного над полем K или кольцо $\boldsymbol{Z}$ целых рациональных чисел, в каждом идеале кольца A можно каноническим образом выбрать образующий: унитарный многочлен кольца $K[x]$ или целое положительное число (§ 1, n°n° 4 и 5). В каждом из этих случаев канонический образующий инвариантного фактора $A\alpha_i$, допуская вольность речи, также называют инвариантным фактором подмодуля M относительно модуля L.

Заметим, что инвариантные факторы подмодуля M относительно модуля L зависят от модуля L, относительно которого M рассматривается как подмодуль; например, все они совпадают с A, если положить $L = M$.

3. Структура модулей конечного типа

Теорема 2. *Всякий модуль конечного типа* E *над кольцом главных идеалов* A *изоморфен прямой сумме конечного числа* m *моногенных модулей* $A/\mathfrak{a}_k$, *где* $\mathfrak{a}_k$ — *идеалы кольца* A (*некоторые из них могут быть нулевыми*) *такие, что* $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_m \neq A$, *причем этими условиями они определяются однозначно.*

Если модуль E порождается q образующими, то он изоморфен фактормодулю L/M, где $L = A^q$ (гл. II, § 1, n° 8, предложение 10). Так как M имеет конечный ранг $n \leqslant q$, то мы находимся в условиях, когда можно применить теорему 1. В обозначениях последней, фактормодуль L/M изоморфен прямой сумме дополнительного подмодуля L' к подмодулю M' в L и модуля кручения M'/M. Модуль L' свободен и имеет конечный ранг $p = q - n$; следовательно, он изоморфен A^p. Если r — наименьший из таких индексов, что $A\alpha_r \neq A$, то фактормодуль M'/M изоморфен прямой сумме модулей $A/A\alpha_i$ при $r \leqslant i \leqslant n$, и условия теоремы выполняются, если положить $m = p + (n - r + 1)$, $\mathfrak{a}_k = (0)$ при $1 \leqslant k \leqslant p$, $\mathfrak{a}_{p+j} = A\alpha_{n-j+1}$ при $1 \leqslant j \leqslant n - r + 1$. Осталось доказать однозначность, но она вытекает из следствия к предложению 2 n° 1.

Следствие 1. *Всякий модуль конечного типа E над кольцом главных идеалов является прямой суммой своего подмодуля кручения и свободного модуля.*

Подмодуль кручения модуля E может, вообще говоря, обладать несколькими различными дополнительными подмодулями. Например, если $E = \mathbf{Z} \times (\mathbf{Z}/(2))$, то подмодуль кручения модуля E есть $\{0\} \times (\mathbf{Z}/(2))$; в качестве дополнительного к нему подмодуля можно взять подмодуль $\mathbf{Z} \times \{0\}$, а также подмодуль, образованный элементами вида $(n, \bar{n})$, где n пробегает $\mathbf{Z}$, а $\bar{n}$ — смежный класс n по mod 2.

В общем случае пусть T — подмодуль кручения модуля E и L_1, L_2 — свободные подмодули E, каждый из которых является дополнительным к T. Пусть $x \to \varphi(x)$ — проекция L_1 на L_2 параллельно T (гл. II, § 1, n° 1). Отображение $x \to \varphi(x) - x$ есть гомоморфизм L_1 на T. Обратно, для любого гомоморфизма $x \to \vartheta(x)$ модуля L_1 на модуль T отображение $x \to x + \vartheta(x)$ есть проекция, параллельная T, модуля L_1 на свободный подмодуль модуля E, дополнительный к T.

Следствие 2. *Над кольцом главных идеалов всякий модуль конечного типа без кручения является свободным модулем конечного ранга.*

Этот результат немедленно вытекает из следствия 1.

Предположение о том, что модуль имеет конечный тип, существенно (см. начало § 3).

Определение 2. *В условиях и обозначениях теоремы 2, идеалы $\mathfrak{a}_k$ называются инвариантными факторами модуля E.*

Как и для определения 1 (n° 2), в случаях, когда $A = \mathbf{Z}$ или $A = K[X]$, канонический образующий идеала $\mathfrak{a}_k$ (целое положительное число или унитарный многочлен), допуская вольность речи, также называют *инвариантным фактором* модуля конечного типа E.

Не следует смешивать инвариантные факторы *модуля* E с инвариантными факторами подмодуля M свободного модуля L *относительно* L (определение 1).

4. Вычисление инвариантных факторов

Предложение 3. *Пусть A — кольцо главных идеалов, L — свободный A-модуль с конечным базисом (u_j) $(1 \leqslant j \leqslant k)$, M — подмодуль L, (x_i) — система образующих M, $A\alpha_i$ $(1 \leqslant i \leqslant n)$ — инвариантные множители M относительно L. Тогда при $1 \leqslant m \leqslant n$ $\delta_m = \alpha_1 \ldots \alpha_m$ есть н. о. д. миноров порядка m матрицы, столбцами которой служат координаты элементов x_i относительно базиса (u_j).*

По теореме 1 имеет место включение $M \subset \alpha_1 L$; следовательно, координаты любого элемента модуля M кратны α_1. С другой стороны, существует элемент $e_1 \in L$, координаты которого независимы в совокупности (следствие теоремы 1) и такой, что $\alpha_1 e_1 \in M$. Поэтому координаты элемента $\alpha_1 e_1$ имеют н. о. д. α_1. Выражая элемент $\alpha_1 e_1$ в виде линейной комбинации элементов x_i, получим, что α_1 является элементом идеала, порожденного координатами x_i. Но все эти координаты делятся на α_1, поэтому α_1 является их н. о. д., и утверждение доказано для случая $m = 1$.

Для доказательства утверждения в случае произвольного m рассмотрим модуль $\overset{m}{\bigwedge} M$, являющийся m-й *внешней степенью* модуля M (гл. III, § 5). В обозначениях теоремы 1, в качестве базиса (a_i) модуля M можно взять элементы $a_i = \alpha_i e_i$ $(1 \leqslant i \leqslant n)$. Следовательно, элементы $a_{i_1} \wedge \ldots \wedge a_{i_m}$ образуют базис модуля $\overset{m}{\bigwedge} M$ ($(i_1, \ldots, i_m)$ пробегает множество строго возрастающих последовательностей из m индексов из отрезка натурального ряда $[1, n]$). Таким образом, элементы $e_{i_1} \wedge \ldots \wedge e_{i_m}$ принадлежат базису B_m модуля $\overset{m}{\bigwedge} L$. Каноническое отображение модуля $\overset{m}{\bigwedge} M$

в модуль $\bigwedge^m L$ является, следовательно, изоморфным отображением модуля $\bigwedge^m M$ на подмодуль модуля $\bigwedge^m L$, обладающий базисом, состоящим из элементов $(\alpha_{i_1} \ldots \alpha_{i_m})\, e_{i_1} \wedge \ldots \wedge e_{i_m}$. Отождествим этот подмодуль с $\bigwedge^m M$. Так как α_j делится на α_k при $j \geqslant k$, то все элементы $\alpha_{i_1} \ldots \alpha_{i_m}$ делятся на $\delta_m = \alpha_1 \ldots \alpha_m$, причем один из них в точности равен δ_m. Следовательно, δ_m есть н. о. д. множества координат образующих модуля $\bigwedge^m M$ относительно базиса B_m модуля $\bigwedge^m L$. Из первой части доказательства получаем, что δ_m есть н. о. д. множества координат любой системы образующих модуля $\bigwedge^m M$ относительно любого базиса модуля $\bigwedge^m L$. Взяв в качестве базиса модуля $\bigwedge^m L$ базис, канонически полученный из базиса (u_j) модуля L, а в качестве системы образующих модуля $\bigwedge^m M$ — систему, образованную внешними произведениями элементов (x_i), и, воспользовавшись выражением координат этих произведений через определители (гл. III, § 6, n° 3), мы закончим доказательство предложения.

5. *Линейные отображения свободных модулей и матрицы над кольцом главных идеалов*

Пусть A — кольцо главных идеалов. Рассмотрим линейное отображение f свободного A-модуля L ранга m в свободный A-модуль L' ранга n. Предыдущие результаты позволяют нам путем надлежащего выбора базисов в L и L' получить матрицу отображения f в наиболее простом виде, который называется *канонической формой* этой матрицы.

Предложение 4. *Пусть A — кольцо главных идеалов и f — линейное отображение ранга r свободного A-модуля L ранга m в свободный A-модуль L' ранга n. Тогда существуют базисы (e_i) $(1 \leqslant i \leqslant m)$ в L и (e'_j) $(1 \leqslant j \leqslant n)$ в L' такие, что $f(e_i) = \alpha_i e'_i$ при $1 \leqslant i \leqslant r$ и $f(e_i) = 0$ при $i > r$; элементы α_i ненулевые, каждый из них делит последующий, и идеалы $A\alpha_i$ являются инвариантными факторами подмодуля $f(L)$ в L' и, следовательно, определяются однозначно.*

Пусть $L_0 = f^{-1}(0)$ — ядро отображения f. Фактормодуль L/L_0 изоморфен подмодулю $f(L)$, который является свободным подмодулем свободного модуля L' (§ 3, теорема 1). Следовательно, L_0 обладает в L дополнением L_1 (гл. II, § 1, n° 6, следствие предложения 4) и сужение f на L_1 является изоморфным отображением L_1 на $f(L) = M'$. Если идеалы $A\alpha_i$ $(1 \leqslant i \leqslant r)$ — инвариантные множители подмодуля M' в L', то по теореме 1 в L' существует базис (e'_j) $(1 \leqslant j \leqslant n)$ такой, что элементы $(\alpha_i e'_i)$ $(1 \leqslant i \leqslant r)$ являются базисом подмодуля M'. Так как сужение f на L_1 есть изоморфизм L_1 на M', то в L_1 существует такой базис (e_i) $(1 \leqslant i \leqslant r)$, что $f(e_i) = \alpha_i e'_i$. Этот базис L_1 можно дополнить элементами базиса (e_s) $(r+1 \leqslant s \leqslant n)$ ядра L_0 до базиса (e_k) $(1 \leqslant k \leqslant n)$ всего модуля L.

Следствие 1. *Пусть X — матрица ранга r из m строк и n столбцов над кольцом главных идеалов A. Тогда существует матрица X_0, эквивалентная X* (гл. II, § 6, n° 10, определение 6) *и имеющая вид*

$$\begin{pmatrix} \alpha_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \alpha_2 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha_r & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix},$$

где α_i — ненулевые элементы кольца A, каждый из которых делит последующий. Этими условиями элементы α_i определяются однозначно с точностью до обратимого множителя.

Говорят, что матрицы X и X' эквивалентны, если существуют такие обратимые квадратные матрицы P и Q над кольцом A, что $X' = PXQ$. Следствие 1 является перефразировкой предложения 4 на матричном языке (см. гл. II, § 6, n° 10).

В обозначениях предложения 4 и следствия 1, ненулевые идеалы $A\alpha_i$ называются *инвариантными факторами* линейного отображения f или матрицы X. Тогда из следствия 1 немедленно получаем

Следствие 2. *Для того чтобы матрицы X и X' из n строк и m столбцов над кольцом главных идеалов A были эквивалентны,*

необходимо и достаточно, чтобы они имели одинаковые инвариантные факторы.

Заметим, что если A — *поле*, то все α_i можно считать равными 1, и мы получили новое доказательство предложения 9 гл. II, § 6, n° 10.

Если X — матрица линейного отображения f относительно некоторого базиса модуля L и некоторого базиса модуля L', то столбцы матрицы X состоят из координат образующих элементов $f(L)$ относительно базиса в L'. Следовательно, из предложения 3 (n° 4) сразу получаем следующий результат:

Предложение 5. *Пусть X — матрица ранга r над кольцом главных идеалов A и $A\alpha_i$ $(1 \leqslant i \leqslant r)$ — ее инвариантные факторы. Тогда α_i есть н. о. д. элементов матрицы X, и, вообще, произведение $\alpha_1 \ldots \alpha_q$ $(q \leqslant r)$ есть н. о. д. миноров порядка q матрицы X.*

6. *Абелевы группы конечного типа*

Абелева группа без операторов (в аддитивной записи) каноническим образом наделяется структурой унитарного модуля над кольцом $\boldsymbol{Z}$ (гл. II, § 1, n° 1); поэтому к ней применимы определения и результаты для модулей над кольцом главных идеалов. Наиболее важным является результат n° 3, который мы для случая $A = \boldsymbol{Z}$ сформулируем заново:

Теорема 3. *Всякая абелева группа G конечного ранга является прямой суммой своей подгруппы кручения F* (подгруппы элементов конечного порядка группы F) *и свободной абелевой группы конечного ранга p* (изоморфной $\boldsymbol{Z}^p$). *Группа F есть прямая сумма конечного числа циклических групп порядков $n_1, n_2, \ldots, n_q$, где $n_i \geqslant 1$ — целые числа, каждое из которых делит предыдущее. Кроме того, целые числа p, q, n_i $(1 \leqslant i \leqslant q)$ однозначно определяются группой G.*

Замечание. В то время как *порядки* $n_1, \ldots, n_q$ циклических групп, в прямую сумму которых разлагается группа F, определяются однозначно условием делимости в теореме 3, этого нельзя сказать о самих циклических группах: например, если группа G есть произведение факторгруппы $\boldsymbol{Z}/(p)$ на самое себя (p — простое), то подгруппы являются подпространствами над полем $\boldsymbol{F}_p$ и группа G может p $(p+1)$ различными способами быть разложена в прямую сумму двух одномерных подпространств.

Следствие 1. *В конечной абелевой группе G существует элемент, порядок которого равен н. о. к. порядков всех элементов группы G. Этот порядок n_1 есть первый инвариантный фактор группы G.*

Следствие 2. *Конечная абелева группа, порядок которой не делится на квадрат целого числа > 1, является циклической.*

В самом деле, порядок такой группы имеет вид $n = p_1 p_2 \ldots p_n$, где p_k $(1 \leqslant k \leqslant m)$ — различные простые числа. Следовательно, p_k-компонента группы G является циклической группой порядка p_k $(1 \leqslant k \leqslant m)$. По следствию 1 в группе G существует элемент порядка n.

7. *Неразложимые модули. Элементарные делители*

Определение 3. *Модуль M над (произвольным) кольцом A называется разложимым, если он представлен в виде прямой суммы двух подмодулей, отличных от M и от $\{0\}$. В противном случае он называется неразложимым.*

Заметим (гл. I, § 6, n° 6), что моногенный модуль $A/\mathfrak{a}$ разложим тогда и только тогда, когда существуют такие идеалы $\mathfrak{b}$ и $\mathfrak{c}$, отличные от $\mathfrak{a}$ и A, что $A = \mathfrak{b} + \mathfrak{c}$ и $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$. Тогда модуль $A/\mathfrak{a}$ изоморфен прямой сумме модулей $A/\mathfrak{b}$ и $A/\mathfrak{c}$. Если A — кольцо целостности, то идеал $\mathfrak{a} = (0)$ этим свойством не обладает, ибо в противном случае произведение любого элемента $x \in \mathfrak{b}$ и любого элемента $y \in \mathfrak{c}$ равно нулю, а это невозможно. Следовательно, кольцо целостности A является неразложимым A-модулем. Если A — кольцо главных идеалов, то $\mathfrak{a} = (a)$, $\mathfrak{b} = (b)$, $\mathfrak{c} = (c)$ и предыдущие условия означают, что a есть н. о. к., а 1 — н. о. д. элементов b и c (§ 1, n° 2, предложение 2). Элемент a ассоциирован тогда с произведением двух независимых элементов b и c (гл. VI, § 1, n° 12, предложение 12 (ДЕЛ)); но это возможно лишь в случае, когда элемент a делится на несколько различных экстремальных элементов. Из сказанного можно заключить, что всякий A-модуль конечного типа разлагается в прямую сумму моногенных подмодулей (n° 3, теорема 2).

Предложение 6. *Для того чтобы модуль конечного типа над кольцом главных идеалов A был неразложим, необходимо и достаточно, чтобы он был изоморфен модулю A или модулю вида $A/(p^n)$, где p — экстремальный элемент кольца A и $n \geqslant 1$ — целое число.*

Теперь ясно, что всякий модуль конечного типа над кольцом главных идеалов является прямой суммой неразложимых модулей. Более точно:

Предложение 7. *Пусть A — кольцо главных идеалов, и P — система представителей экстремальных элементов кольца A. Всякий A-модуль конечного типа E разлагается в прямую сумму неразложимых подмодулей конечного типа. Для такого разложения обозначим через $m(0)$ число неразложимых подмодулей, изоморфных A, и для всякого элемента p^n ($p \in P$, $n \geqslant 1$ — целое число) обозначим через $m(p^n)$ число неразложимых подмодулей, изоморфных $A/(p^n)$. Тогда числа $m(0)$ и $m(p^n)$ не зависят от рассматриваемого разложения.*

В самом деле, модуль E является прямой суммой своего модуля кручения M (который определяется однозначно) и свободного модуля, изоморфного A^q (n° 3, следствие 1 теоремы 2). Целое число $q = m(0)$ определяется однозначно, так как оно равно рангу свободного модуля E/M.

Докажем теперь, что модуль кручения M есть прямая сумма неразложимых модулей конечного типа. Нам потребуется следующая лемма:

Лемма 2. *Если A — кольцо главных идеалов, то любой подмодуль моногенного модуля сам является моногенным.*

В самом деле, любой подмодуль моногенного A-модуля $A/(a)$ имеет вид $(d)/(a)$, где d делит a; следовательно, он порождается смежным классом элемента d по mod a.

Рассмотрим каноническое разложение модуля M в прямую сумму его p-компонент M_p (§ 2, теорема 1) и некоторое разложение модуля M в прямую сумму моногенных подмодулей N_i (n° 3, теорема 2). По следствию теоремы 1 § 2 модуль N_i есть прямая сумма подмодулей $N_i \cap M_p$ (p пробегает множество P). По лемме 2 каждый из модулей $N_i \cap M_p$ моногенный, и поскольку его аннулятор имеет вид (p^n), то модуль $N_i \cap M_p$ изоморфен фактормодулю $A/(p^n)$.

Докажем, наконец, что числа $m(p^n)$ определяются однозначно. Так как M—модуль конечного типа, то он не может быть разложен в бесконечную прямую сумму подмодулей, отличных от $\{0\}$: каждый из образующих элементов модуля M в любом прямом раз-

ложении M имеет конечное число компонент $\neq 0$. Следовательно, в каждом разложении модуля M в прямую сумму неразложимых подмодулей имеется лишь конечное число подмодулей, изоморфных $A/(p^n)$. Обозначим через F_p сумму всех неразложимых подмодулей такого разложения, являющихся p-модулями. Ясно, что $F_p \subset M_p$, и так как модуль M является, с одной стороны, прямой суммой подмодулей F_p, а с другой стороны, прямой суммой подмодулей M_p (p пробегает множество P), то $F_p = M_p$ при любом $p \in P$. Наконец, так как модуль F_p есть прямая сумма конечного числа подмодулей, изоморфных модулям вида $A/(p^n)$, и множество идеалов (p^n) $(n \geqslant 1)$ совершенно упорядоченно по включению, то единственность чисел $m(p^n)$ вытекает из следствия предложения 2.

Определение 4. *В обозначениях предложения 7, идеалы* (p^n) $(p \in P,\ n \geqslant 1$ — *целое число*), *для которых* $m(p^n) > 0$, *называются элементарными делителями модуля* E, *а целые числа* $m(p^n)$ — *их кратностями. Если число* $m(0) > 0$, *то оно называется кратностью нулевого элементарного делителя.*

Как и для инвариантных множителей (n° 2, определение 1), в случае, когда $A = \mathbf{Z}$ или $A = K[X]$ (K — поле), канонический образующий идеала (p^n) (целое положительное число или унитарный многочлен), допуская вольность речи, также называют *элементарным делителем модуля* конечного типа E.

Замечания. 1) Если E — конечная абелева группа, то ее структуру можно описать, выписав последовательно ее элементарные делители, каждый столько раз, какова его кратность. Говорят, например, что группа G есть группа «типа (2, 2, 4, 27, 27, 25)» (или просто «группа (2, 2, 4, 27, 27, 25)»), если она изоморфна произведению двух групп $\mathbf{Z}/(2)$, одной группы $\mathbf{Z}/(2^2)$, двух групп $\mathbf{Z}/(3^3)$ и одной группы $\mathbf{Z}/(5^2)$.

2) Если модуль кручения E конечного типа над кольцом главных идеалов A задан как прямая сумма моногенных модулей, изоморфных фактормодулям $A/(a_i)$ (в частности, если известны его инвариантные множители), то можно найти его элементарные делители, а следовательно, и их кратности, заметив, что факторкольцо $A/(a)$ изоморфно произведению факторколец $A/(p^{n(p)})$, где $a = \varepsilon \prod_{p \in P} p^{n(p)}$ — разложение элемента a на экстремальные множители (§ 1, предложение 4). Рассмотрим в качестве примера мультипликативную группу G (464600) обратимых элементов кольца $\mathbf{Z}/(464600)$ (§ 2, n° 4). Так как

$464600 = 2^3 \cdot 5^2 \cdot 23 \cdot 101$, то эта группа изоморфна произведению групп $G(2^3)$, $G(5^2)$, $G(23)$ и $G(101)$ (§ 2, теорема 3). Последние три группы циклические, и их порядки 20, 22 и 100, а группа $G(2^3)$ является произведением двух циклических групп второго порядка (там же); так как $20 = 2^2 \cdot 5$, $22 = 2 \cdot 11$ и $100 = 2^2 \cdot 5^2$, то группа (464600) имеет тип $(2, 2, 2, 2^2, 2^2, 5, 5^2, 11)$.

3) Для вычисления инвариантных факторов модуля кручения по известным элементарным делителям снова будем опираться на тот факт, что если элементы a_i кольца A попарно независимы, то произведение $\prod_i A/(a_i)$ является моногенным модулем, изоморфным $A/(a_1 a_2 \ldots a_n)$ (§ 1, предложение 4). Способ вычисления продемонстрируем на примере группы $G(464600)$: элементарные делители p^n группы G, относящиеся к одному экстремальному элементу p, записываются в одну строчку, начиная с элементарных делителей наивысшей степени; каждая полученная таким образом строчка дополняется (если это необходимо) единицами, с тем чтобы все строки имели одинаковую длину:

$$2^2,\ 2^2,\ 2,\ 2,\ 2$$
$$5^2,\ 5,\ 1,\ 1,\ 1$$
$$11,\ 1,\ 1,\ 1,\ 1$$

Тогда инвариантные факторы являются произведениями элементов, стоящих в одном столбце: 1100, 20, 2, 2, 2. В самом деле, группа G изоморфна произведению циклических групп порядков 1100, 20, 2, 2, 2 в силу предложения 4 § 1, и поскольку каждый из этих порядков делится на следующий, то эти порядки являются инвариантными множителями группы G (теорема 3).

Упражнения. 1) Пусть $U = (\alpha_{ij})$ — матрица из m строк и n столбцов над кольцом главных идеалов A.

а) Предположим сначала, что элементы α_{ij} независимы в совокупности. Показать, что существуют обратимые матрицы P и Q с элементами из кольца A такие, что матрица PAQ равна единице. (Для каждого $\alpha_{ij} \neq 0$ пусть $s(\alpha_{ij})$ — сумма показателей степеней в разложении α_{ij} на экстремальные элементы и $s(U)$ — наименьшее из чисел $s(\alpha_{ij})$ показать, что если $s(U) > 0$, то существуют такие обратимые матрицы R, S, что $s(RUS) < s(U)$; воспользоваться тождеством Безу; применяя при необходимости перестановки строк или столбцов, ограничиться лишь такими матрицами R и S, которые имеют вид $\begin{pmatrix} T & 0 \\ 0 & I \end{pmatrix}$, где T — матрица порядка 2, I — единичная матрица, или являются произведением таких матриц и матриц перестановок.)

б) Пусть δ_1 — н. о. д. элементов матрицы U. Показать, что существуют такие обратимые матрицы P_1, Q_1, что

$$P_1 U Q_1 = \begin{pmatrix} \delta_1 & 0 \\ 0 & U_1 \end{pmatrix},$$

где все элементы матрицы U_1 делятся на δ_1 (использовать а) и преобразования, состоящие в прибавлении к некоторой строке (или столбцу) некоторого кратного другой строки (соответственно столбца)).

в) Получить из б) способ явного вычисления инвариантных факторов матрицы с элементами из кольца $A = \boldsymbol{Z}$. Применить этот способ к матрице

$$\begin{pmatrix} 6 & 8 & 4 & 20 \\ 12 & 12 & 18 & 30 \\ 18 & 4 & 4 & 10 \end{pmatrix}.$$

2) Пусть A — кольцо главных идеалов. Для того чтобы два подмодуля M и N модуля A^q переводились друг в друга некоторым автоморфизмом модуля A^q, необходимо и достаточно, чтобы их инвариантные факторы относительно A^q совпадали.

3) Пусть A — кольцо главных идеалов, K — его поле дробей, E — векторное пространство над K, M — A-модуль конечного типа ранга n, содержащийся в E, N — A-модуль конечного типа ранга $p \leqslant n$, содержащийся в KM. Показать, что существуют базисы $(e_i)_{1 \leqslant i \leqslant n}$ модуля M и $(\alpha_i e_i)$ $(1 \leqslant i \leqslant p)$ модуля N такие, что $\alpha_i \in K$ и α_i делит α_{i+1} (относительно кольца A) при $1 \leqslant i \leqslant p - 1$; показать, кроме того, что дробные идеалы $A\alpha_i$ определяются однозначно (*инвариантные факторы N относительно M*) (заметить, что существует $\beta \in K$ такое, что $N \subset \beta M$).

4) Пусть G — конечная абелева группа.

а) Показать, что для любого простого числа p число элементов группы G, имеющих порядок p, равно $p^N - 1$, где $N = \sum_{n=1}^{\infty} m\,(p^n)$.

б) Вывести отсюда, что если уравнение $x^p = 1$ при любом простом p имеет не более p решений в группе G, то G — циклическая группа.

5) Пусть G — конечная абелева группа порядка n. Показать, что для любого целого делителя q числа n в группе G существует подгруппа порядка q (разложить G в прямую сумму неразложимых циклических групп).

*6) Пусть A — коммутативное кольцо с единицей и E — унитарный A-модуль. Обозначим через $\mathscr{E}$ кольцо эндоморфизмов абелевой группы (без операторов) E; для любого подкольца $B \subset \mathscr{E}$ через B' обозначим коммутант B в $\mathscr{E}$ (подкольцо, состоящее из элементов $\mathscr{E}$, перестановочных со всеми элементами подкольца B).

а) Пусть A_0 — подкольцо кольца $\mathscr{E}$, состоящее из гомотетий $x \to \lambda x$ $(\lambda \in A)$; известно, что подкольцо A_0 изоморфно факторкольцу $A/\mathfrak{a}$, где $\mathfrak{a}$ — аннулятор модуля E, и его коммутант A_0' в кольце $\mathscr{E}$ является кольцом эндоморфизмов $\mathscr{L}(E)$ A-модуля E (гл. II, §§ 1 и 2). Показать, что коммутант A_0'' кольца A_0' коммутативен, а его коммутант $A_0''' = A_0'$ (заметить, что $A_0 \subset A_0'$).

б) Показать, что если подмодуль F модуля E обладает дополнением, то $u(F) \subset F$ для любого $u \in A_0''$ (рассмотреть проекцию модуля E на F при разложении E на прямую сумму F и другого подмодуля).

в) Пусть модуль E является прямой суммой семейства (F_ι) моногенных подмодулей. Показать, что при $u \in A_0''$ для всякого индекса ι существует элемент $\alpha_\iota \in A$ такой, что $u(x) = \alpha_\iota x$ для всех $x \in F_\iota$ (использовать б)).

г) Пусть модуль E является прямой суммой последовательности (E_n) (конечной или бесконечной) моногенных модулей, такой, что последовательность $(\mathfrak{b}_n)$, где $\mathfrak{b}_n$ — аннулятор модуля E_n, возрастает. Показать, что $A_0'' = A_0$ (использовать в), а также тот факт, что для любого $i > 1$ существует эндоморфизм $v_i \in \mathscr{E}(E) = A_0'$, переводящий E_{i-1} в E_i).

Рассмотреть применение к случаю, когда A — кольцо главных идеалов и E — модуль конечного типа над A.

7) Пусть A — кольцо главных идеалов, K — его поле дробей, E — модуль без кручения конечного типа ранга n над кольцом A, E^* — его сопряженный модуль (гл. II, § 4, n° 1); модули E и E^* оба изоморфны A^n.

а) Пусть M — подмодуль в E, M^0 — подмодуль в E^*, ортогональный к M (гл. II, § 4, n° 2); показать, что модуль E^*/M^0 без кручения и, следовательно, M^0 обладает в E^* дополнением; подмодуль M^{00} модуля E, ортогональный к M^0, совпадает с $E \cap KM$ (при этом модуль E рассматривается канонически погруженным в векторное пространство размерности n над K). Модуль E^*/M^0 можно рассматривать как канонически погруженный в сопряженный к M модуль M^* (гл. II, § 4, упражнение 4); показать, что инвариантные факторы E^*/M_0 относительно M^* равны инвариантным факторам подмодуля M относительно E (воспользоваться теоремой 1).

б) Пусть F — еще один модуль без кручения конечного типа над кольцом A и u — линейное отображение модуля E в F. Показать, что инвариантные факторы модуля ${}^tu(F^*)$ относительно E^* совпадают с инвариантными факторами $u(E)$ относительно F (поступить так же, как в предложении 4).

8) Пусть G — модуль кручения конечного типа над кольцом главных идеалов A и M и N — свободные модули, такие, что $N \subset M$, и модуль G изоморфен M/N; инвариантные факторы модуля N относительно M, отличные от A, совпадают с инвариантными факторами модуля G (теорема 2); их число называется рангом модуля G.

а) Показать, что ранг r модуля G является наименьшим числом его моногенных подмодулей, прямая сумма которых равна G, и равен наибольшему из рангов π-компонент модуля G.

б) Показать, что ранг любого подмодуля и любого фактормодуля модуля G не превосходит ранга G (рассмотреть G как фактормодуль двух свободных модулей ранга r).

в) Показать, что при любом $\lambda \in A$ ранг подмодуля λG равен числу инвариантных факторов модуля G, не делящих λ (заметить, что модуль λE, где $E = A/(A\alpha)$, изоморфен $(A\lambda)/((A\alpha) \cap (A\lambda))$). Вывести отсюда, что k-й инвариантный фактор модуля G (если эти идеалы расположены в *убывающем* порядке) является н. о. д. тех $\lambda \in A$, для которых ранг модуля λG не превосходит $r - k$.

г) Пусть $A\alpha_k$ $(1 \leqslant k \leqslant r)$ — инвариантные факторы модуля G, расположенные в убывающем порядке, H — подмодуль в G ранга $r - q$, $A\beta_k$ $(1 \leqslant k \leqslant r - q)$ — его инвариантные факторы, расположенные в убывающем порядке. Вывести из б) и в), что при $1 \leqslant k \leqslant r - q$ β_k делит α_{k+q}. Аналогично показать, что если модуль G/H имеет ранг $r - p$ и $A\gamma_k$ $(1 \leqslant k \leqslant r - p)$ — его инвариантные факторы, расположенные в убывающем порядке, то при $1 \leqslant k \leqslant r - p$ γ_k делит α_{k+p}.

д) Обратно, пусть L — модуль кручения ранга $r - q$, $A\lambda_k$ $(1 \leqslant k \leqslant r - q)$ — его инвариантные факторы и λ_k делит α_{k+q} при $1 \leqslant k \leqslant r - q$. Показать, что в G существуют подмодули M и N такие, что модуль L изоморфен M и G/N (разложить G в прямую сумму подмодулей, изоморфных $A/A\alpha_k$).

*9) Пусть A — кольцо главных идеалов, K — его поле дробей, E — векторное пространство над K, M — A-модуль конечного типа ранга n, содержащийся в E, N — A-модуль конечного типа ранга p, содержащийся в KM, P — M-модуль конечного типа ранга q, содержащийся в KN.

а) Пусть $A\alpha_i$ $(1 \leqslant i \leqslant p)$ — инвариантные факторы модуля N относительно M, расположенные в убывающем порядке (упражнение 3). Показать, что при $1 \leqslant k \leqslant p$ элемент α_k является н. о. д. таких элементов $\lambda \in K$, для которых ранг фактормодуля $(N + \lambda (KN \cap M))/N$ не превосходит $p - k$ (см. упражнение 8г)).

б) Пусть $A\beta_i$ $(1 \leqslant i \leqslant q)$ — инвариантные факторы модуля P относительно N, $A\gamma_j$ $(1 \leqslant j \leqslant p)$ — инвариантные факторы P относительно N, расположенные в убывающем порядке. Показать, что при $1 \leqslant j \leqslant q$ $\alpha_1\gamma_j$ делит β_j (см. упражнение 8).

в) Показать, что при $1 \leqslant j \leqslant q$ $\gamma_1\alpha_j$ делит β_j. (Рассмотреть сначала случай $n = p = q$ и применить упражнение 8. В общем случае показать, что всегда можно предполагать $p = n$, и рассмотреть в M подмодуль Q такой, что $P + \varrho Q$ при любом $\varrho \in A$ имеет ранг p; затем взять достаточно маленький идеал $A\varrho$ и применить предложение 3.)

г) Пусть H — подмодуль в N ранга $k \leqslant p$ и (μ_H) — дробный идеал, состоящий из элементов $\mu \in K$ таких, что $\mu (M \cap KH) \subset H$. Вывести из в), что α_k при любом k, $1 \leqslant k \leqslant p$, является н. о. д. элементов μ_H, когда H пробегает множество подмодулей ранга k модуля N.

*10) Пусть A — кольцо главных идеалов, M — подмодуль ранга n модуля $E = A^n$ и $A\alpha_i$ $(1 \leqslant i \leqslant n)$ — инвариантные факторы модуля M относительно E, расположенные в убывающем порядке.

Пусть N — подмодуль M, обладающий в M дополнением (то есть $N = M \cap KN$, где K — поле дробей кольца).

а) Пусть P — дополнение модуля N в M. Показать, что подмодуль $(P + (E \cap KN))/M$ модуля E/M изоморфен $(E \cap KN)/N$. Вывести отсюда, что если ранг модуля N равен p и $A\beta_k$ $(1 \leqslant k \leqslant p)$ — его инвариантные факторы относительно E, то при $1 \leqslant k \leqslant p$ β_k делит α_{k+n-p} (воспользоваться упражнением 8г)).

б) Привести пример, показывающий, что модуль E/M не обязательно изоморфен произведению модулей $(E \cap KN)/N$ и $E/(P + (E \cap KN))$ (взять случай, когда E/M неразложим).

*11) Пусть A — кольцо главных идеалов, H — подмодуль в $E = A^n$ ранга $k - 1$, обладающий в E дополнением (то есть $H = E \cap KH$), и H^0 — подмодуль сопряженного к E модуля E^*, ортогональный к H (упражнение 7); пусть (ν_H) — н. о. д. идеалов $f(M)$ кольца A, где f пробегает H^0; показать, что если H пробегает множество подмодулей ранга $k - 1$ модуля E, обладающих дополнением в E, то α_k при любом k $(1 \leqslant k \leqslant p)$ является н. о. к. элементов ν_H (рассмотреть сначала случай $k = 1$; результат применить к подмодулю $(M + H)/H$ модуля E/H и воспользоваться упражнением 8г), примененным к фактормодулю $E/(M + H)$ модуля E/M).

12) Пусть G' — модуль кручения конечного типа над кольцом главных идеалов. Показать, что его подмодуль H не может быть изоморфным G, не будучи ему равным (заметить, что подмодули модуля G удовлетворяют условию минимальности (§ 2, упражнение 5), и применить упражнение 15, гл. I, § 6).

*13) Пусть M — модуль кручения конечного типа над кольцом главных идеалов A. *Приведенным сопряженным модулем* модуля M называется модуль, сопряженный к *точному* модулю, ассоциированному с M (см. исправления к выпуску VI). Этот модуль также обозначается через M^*.

а) Показать, что модуль M^*, рассматриваемый как A-модуль, изоморфен модулю линейных отображений модуля M в A-модуль K/A (см. § 2, п° 3); эти отображения называются *характерами* модуля M.

б) Показать, что если элементы α, $\beta \in A$ не равны 0, то модуль линейных отображений $A/(\alpha)$ в $A/(\beta)$ изоморфен A (δ), где δ — н. о. д. α и β (гл. II, § 2, упражнение 2). Вывести отсюда, что приведенный сопряженный модуль M^* модуля M *изоморфен* M и каноническое отображение модуля M в M^{**} является изоморфизмом M на M^{**} (применить упражнение 12).

в) Пусть N — подмодуль в M, N^0 — подмодуль в M^*, ортогональный к N, N^{00} — подмодуль в M, ортогональный к N^0; показать, что $N^{00} = N$ и что модуль, сопряженный к N, отождествляется с M^*/N^0 (заметив, что модуль, сопряженный к N, содержит M^*/N^0, а модуль, сопряженный к M^*/N^0, равен N^{00} и содержит N, применить упражнение 12).

г) Применяя в), распространить на модули кручения конечного типа над кольцом главных идеалов теорию линейных уравнений над телом, развитую в гл. II, § 4, n° 8.

д) Вывести из б) и в), что для любого подмодуля N модуля M в M найдется подмодуль P такой, что M/N изоморфен P, а M/P изоморфен N; два подмодуля M, обладающие этими свойствами, называются *взаимными*. Показать, что при любом $\alpha \in A$ подмодуль $M(\alpha)$, состоящий из элементов $x \in M$ таких, что $\alpha x = 0$, и подмодуль αM взаимны.

*14) Пусть M — модуль кручения конечного типа над кольцом главных идеалов A.

а) Показать, что для любого его подмодуля N ранг n модуля M не превосходит суммы рангов модулей N и M/N. (Пусть $M = E/H$, где E — свободный модуль ранга n и H — его подмодуль ранга n; пусть $N = L/H$, где $H \subset L \subset E$; заметить, что если ранг модуля N равен p, то в H существует подмодуль R ранга $n - p$, обладающий в L дополнением S, и $S \cap H = R$ является его дополнением в H; кроме того, модуль $(E \cap KR)/R$ имеет ранг $\geqslant n - p$ и изоморфен фактормодулю модуля E/L (упражнение 10а)); в заключение воспользоваться упражнением 8б).)

б) Пусть N — подмодуль модуля M ранга p, и пусть q — ранг фактормодуля M/N. Пусть $A\alpha_i$ $(1 \leqslant i \leqslant n)$ — инвариантные факторы модуля M, а $A\beta_k$ $(1 \leqslant k \leqslant p)$ — инвариантные факторы модуля M, расположенные в порядке возрастания. Показать, что при $1 \leqslant k \leqslant p$ элемент β_k делится на $\alpha_{k-(p+q-n)}$ (использовать а) и упражнение 8в), заметив, что $(\lambda M)/(\lambda N)$ изоморфен фактормодулю модуля M/N).

15) а) Пусть M — модуль кручения конечного типа ранга n над кольцом главных идеалов A, и $A\alpha_i$ $(1 \leqslant i \leqslant n)$ — его инвариантные множители, расположенные в убывающем порядке. Пусть (β_i) $(1 \leqslant i \leqslant n)$ — некоторая последовательность элементов кольца A такая, что при $1 \leqslant i \leqslant n$ β_i делит α_i и при $1 \leqslant i \leqslant n-1$ α_i делит β_{i+1}. Пусть (M_i) — последовательность подмодулей модуля M такая, что $M_{1 \leqslant i \leqslant n}$ является прямой суммой M_i и M_i изоморфен $A/A\alpha_i$ $(1 \leqslant i \leqslant n)$; пусть a_i — образующий модуля M_i $(1 \leqslant i \leqslant n)$. Положим

$$b = \beta_1 a_1 + \frac{\beta_1\beta_2}{\alpha_1} a_2 + \frac{\beta_1\beta_2\beta_3}{\alpha_1\alpha_2} a_3 + \ldots + \frac{\beta_1\beta_2 \ldots \beta_n}{\alpha_1\alpha_2 \ldots \alpha_{n-1}} a_n.$$

Показать, что фактормодуль модуля M по моногенному подмодулю Ab изоморфен прямой сумме n модулей $A/A\beta_i$ $(1 \leqslant i \leqslant n)$.

б) Пусть M и N — модули кручения конечного типа над кольцом A, $A\alpha_i$ $(1 \leqslant i \leqslant n)$ и $A\beta_k$ $(1 \leqslant k \leqslant p)$ — инвариантные факторы соответственно модулей M и N, расположенные в убывающем порядке; предположим, что $p \leqslant n$, β_k делит α_{k+n-p} при $1 \leqslant k \leqslant p$ и α_k делит $\beta_{k+(p+q-n)}$ при $1 \leqslant k \leqslant n - q$, где q — целое число такое, что $q \leqslant n \leqslant p + q$. Показать, что в модуле M существует подмодуль P, изоморфный N и такой, что ранг M/P не превосходит q (разложить модули M и N в прямую сумму q модулей, сводя, таким

образом, доказательство к случаю $q = 1$; затем применить а) и упражнение 13д)).

в) Для того чтобы модуль N над кольцом A был изоморфен подмодулю модуля кручения M конечного типа, обладающему в M дополнением, необходимо и достаточно, чтобы всякий элементарный делитель N был элементарным делителем M и его кратность в N не превосходила его кратности в M. Получить отсюда пример модуля кручения M конечного типа и его подмодуля N такого, что ранг M равен сумме рангов модулей N и M/N, но N не обладает в M дополнением (использовать а)).

16) Пусть M — модуль над коммутативным кольцом A. Подмодуль N модуля M называется *характеристическим*, если $u(N) \subset N$ для любого эндоморфизма u модуля M. Для любого $\alpha \in A$ подмодуль $M(\alpha)$ элементов $x \in M$, аннулирующихся элементом α, и подмодуль αM являются характеристическими подмодулями.

а) Показать, что если N — характеристический подмодуль в M и P и Q — дополнительные подмодули в M, то N является прямой суммой $N \cap P$ и $N \cap Q$ (рассмотреть проекции модуля M на P и Q).

б) Пусть M — модуль кручения конечного типа над кольцом главных идеалов A; пусть $A\alpha_i$ — инвариантные факторы модуля M, расположенные в убывающем порядке ($1 \leqslant i \leqslant n$); пусть $(M_i)_{1 \leqslant i \leqslant n}$ — последовательность подмодулей модуля M такая, что M является прямой суммой M_i, и каждый модуль M_i изоморфен $A/A\alpha_i$ при $1 \leqslant i \leqslant n$. Пусть N — характеристический подмодуль в M, и $A\beta_i$ — аннулятор $N \cap M_i$ ($1 \leqslant i \leqslant n$); положив $\alpha_i = \beta_i\gamma_i$, показать, что при $1 \leqslant i \leqslant n-1$ β_i делит β_{i+1} и γ_i делит γ_{i+1} (заметить, что при $1 \leqslant i \leqslant n-1$ существует эндоморфизм модуля M, переводящий M_i в M_{i+1}).

в) Обратно, пусть N — подмодуль в M, являющийся прямой суммой подмодулей $N_i \subset M_i$; предположим, что аннуляторы $A\beta_i$ подмодулей N_i ($1 \leqslant i \leqslant n$) удовлетворяют предыдущим условиям. Показать, что N — характеристический подмодуль в M. Вывести отсюда, что если характеристические подмодули модуля M имеют одинаковые инвариантные факторы, то они совпадают.

17) Пусть A — кольцо главных идеалов, элемент $\alpha \in A$ отличен от 0, E — модуль A/A_α. Произведение E^n изоморфно $A^n/\alpha A^n$.

а) Пусть u — линейное отображение E^n в E^m; показать, что u может быть получено путем факторизации из некоторого линейного отображения v произведения A^n в A^m.

б) Пусть $A\beta_i$ ($1 \leqslant i \leqslant p \leqslant \mathrm{Min}(m, n)$) — инвариантные факторы модуля $v(A^n)$ относительно A^m, расположенные в убывающем порядке, $q \leqslant p$ — наибольший из индексов i таких, что α не делит β_i, и δ_i — н. о. д. элементов α и β_i, $1 \leqslant i \leqslant q$. Показать, что ядро $u^{-1}(0)$ отображения u является прямой суммой $n - q$ модулей, изоморфных E, и q моногенных модулей, изоморфных соответственно модулям $A/A\delta_i$

$(1 \leqslant i \leqslant q)$. Положив $\alpha = \gamma_i\delta_i$ $(1 \leqslant i \leqslant q)$, показать, что $A\gamma_i$ являются инвариантными факторами модуля $u(E^n)$.

18) Пусть C — кольцо главных идеалов. Рассмотрим систему линейных уравнений $\sum_{j=1}^{n} \alpha_{ij}\xi_j = \beta_i$ $(1 \leqslant i \leqslant m)$, все коэффициенты и правые части которой принадлежат C, и обозначим через A матрицу (α_{ij}) из m строк и n столбцов и через B — матрицу, полученную из A добавлением $(n+1)$-го столбца (β_i). Показать, что рассматриваемая система имеет по крайней мере одно решение (ξ_j) в C^n тогда и только тогда, когда выполняются следующие условия: 1° матрицы A и B имеют одинаковый ранг p; 2° некоторый н. о. д. миноров порядка p матрицы A равен некоторому н. о. д. миноров поряда p матрицы B (использовать предложение 3 и упражнение 9в)).

19) Пусть C — кольцо главных идеалов. Рассмотрим систему «линейных конгруэнций» $\sum_{j=1}^{n} \alpha_{ij}\xi_j \equiv \beta_i \pmod{\alpha}$, где коэффициенты, правые части и элемент α принадлежат C; обозначим через A матрицу (α_{ij}), через B — матрицу, полученную из A добавлением столбца (β_i), через δ_k (соответственно δ'_k) — некоторый н. о. д. миноров порядка k матрицы A (соответственно B). Рассматриваемая система имеет по крайней мере одно решение в C^n тогда и только тогда, когда:

а) при $m \leqslant n$ п. о. д. элементов α^m, $\alpha^{m-1}\delta_1$, . . ., $\alpha\delta_{m-1}$, δ_m является н. о. д. элементов α^m, $\alpha^{m-1}\delta'_1$, . . ., $\alpha\delta'_{m-1}$, δ'_m;

б) при $m > n$ н. о. д. элементов α^{n+1}, $\alpha^n\delta_1$, . . ., $\alpha\delta_n$ является н. о. д. элементов α^{n+1}, $\alpha^n\delta'_1$, . . ., $\alpha\delta'_n$.

(Свести систему линейных конгруэнций к системе линейных уравнений и использовать упражнение 18.)

20) а) Пусть C — кольцо главных идеалов и

$$f(x_1, x_2, \ldots, x_p) = \sum_{(i_k)} \alpha_{i_1 i_2 \ldots i_p} \xi_{1, i_1} \xi_{2, i_2} \cdots \xi_{p, i_p}$$

— p-линейная форма, определенная в E^n, где E — C-модуль C^n (ξ_{ij} — координата с номером j элемента x_i). Показать, что если δ — н. о. д. коэффициентов $\alpha_{i_1 i_2 \ldots i_p}$, то существует точка $(a_k) \in E^p$ такая, что $f(a_1, a_2, \ldots, a_p) = \delta$ (свести доказательство к случаю $\delta = 1$ и, используя теорему 1, провести индукцию по p).

б) Пусть α_i $(1 \leqslant i \leqslant n)$ — n элементов кольца C, и δ — их н. о. д. Показать, что существует квадратная матрица A порядка n над кольцом C, правый столбец которой равен (α_i), а определитель равен δ (использовать а)).

21) Пусть C — кольцо главных идеалов, $A = (\alpha_{ij})$ — квадратная матрица порядка n над C.

а) Показать, что над кольцом C существует квадратная матрица U порядка n с определителем 1 такая, что первые $n-1$ элементов

последнего столбца матрицы UA равны нулю, а n-й является н. о. д. элементов n-го столбца матрицы A (использовать упражнение 20б)).

б) Вывести отсюда, что над кольцом C существует квадратная матрица порядка V с определителем, равным 1, такая, что все элементы матрицы $VA = (\beta_{ij})$, лежащие выше диагонали, равны нулю («приведенная» эрмитова форма матрицы A).

в) Пусть W — квадратная матрица над кольцом C порядка n с определителем, равным 1, и все элементы матрицы $WA = (\gamma_{ij})$, лежащие выше диагонали, равны нулю; показать, что при $1 \leqslant i \leqslant n$ элементы β_{ii} и γ_{ii} ассоциированы.

*22) Говорят, что модуль M над кольцом главных идеалов A есть модуль *конечного ранга*, если существует целое число $m > 0$, обладающее следующими свойствами: всякий подмодуль конечного типа модуля M содержится в некотором подмодуле M, имеющем систему образующих из не более чем m элементов. Наименьшее число m, обладающее этим свойством, называется *рангом* модуля m.

а) Показать, что если модуль M конечного ранга, то всякий его фактормодуль конечного ранга и его ранг не превосходит ранга модуля M.

б) Для модуля без кручения M понятие ранга, определенное выше, совпадает с понятием ранга, определенным в § 3.

в) Показать, что если модуль M конечного ранга, то всякий его подмодуль конечного ранга и его ранг не превосходит ранга модуля M.

г) Пусть M — π-модуль и $M(\pi) = M$. Показать, что если модуль M конечного ранга, то он конечного типа.

д) Пусть M — π-модуль без элементов конечной высоты. Показать, что если модуль M конечного ранга, то он конечного типа и понятие ранга совпадает с понятием, определенным в упражнении 8. (Заметить, что если $M(\pi)$ конечного типа, то и M конечного типа, доказав для этого, что высоты в M элементов $M(\pi)$ ограничены; для этого использовать упражнение 5 § 2.)

е) Пусть M — π-модуль ранга r, M_0 — его подмодуль, состоящий из элементов, имеющих в M бесконечную высоту. Показать, что M_0 — делимый модуль, прямая сумма конечного числа p неразложимых подмодулей U_π (§ 2, упражнение 3), и модуль M является прямой суммой M_0 и подмодуля N конечного типа и ранга $r - p$. (С помощью д) заметить, что модуль M/M_0 конечного типа; затем применить упражнение 3 § 2.)

ж) Вывести из предыдущего, что модуль M имеет конечный ранг r тогда и только тогда, когда его фактормодуль M/T по подмодулю кручения T имеет конечный ранг $p \leqslant r$, каждая из π-компонент подмодуля T имеет ранг $\leqslant r - p$ и по крайней мере одна из них имеет ранг $r - p$.

з) Пусть (p_n) — последовательность различных простых чисел, пусть E — $\boldsymbol{Z}$-модуль, прямая сумма моногенных подмодулей $\boldsymbol{Z}/(p_n^2)$,

и e_n — элемент модуля E, все координаты которого, отличные от n-й, равны нулю, а n-я координата равна классу 1 по mod p_n^2. Пусть M — подмодуль $\mathbf{Z}$-модуля $E \times \mathbf{Q}$, порожденный элементами $(e_n, 1/p_n)$. Показать, что M — модуль ранга 2, его подмодуль кручения T порождается элементами $(p_n e_n, 0)$ и не имеет в M дополнения. (Пусть $\bar{x}_n$ — класс элемента $(e_n, 1/p_n)$ по модулю T; показать, что при любом $m \neq n$ существует класс $\bar{y}_{nm}$ по модулю T такой, что $\bar{x}_n = p_m \bar{y}_{nm}$, но в классе $\bar{x}_n$ не существует элемента x_n такого, что при любом $m \neq n$ существует элемент $y_{nm} \in M$ такой, что $x_n = p_m y_{nm}$.)

§ 5. Эндоморфизмы векторных пространств

Обозначения. Пусть даны модуль E, элемент $x \in E$ и эндоморфизмы u и v модуля E; в этом параграфе вместо $u(x)$, $(u \circ v)(x)$, $u \circ v$ мы будем писать соответственно ux, uvx, uv. Через 1 мы будем обозначать тождественное отображение модуля E на себя в случаях, когда это не может привести к недоразумению.

1. *Модуль, ассоциированный с эндоморфизмом*

Пусть E — векторное пространство конечной размерности n над полем K, и u — его эндоморфизм. Рассмотрим кольцо $K[X]$ многочленов от одного переменного X над полем K. Для любого многочлена $p(X) \in K[X]$ и любого элемента $x \in E$ положим

$$p(X)\,x = p(u)\,x. \tag{1}$$

Тем самым определено билинейное отображение произведения $K[X] \times E$ в E, задающее на E структуру *унитарного* $K[X]$*-модуля*. Множество E, наделенное этой структурой, обозначается далее через E_u. Заданная на E структура векторного пространства получается из E_u сужением его кольца операторов до K.

Обратно, всякий унитарный $K[X]$-модуль E', являющийся конечномерным векторным пространством над K, может быть получен этим способом; это следует из коммутативности кольца $K[X]$: достаточно рассмотреть эндоморфизм u, определенный равенством $ux = Xx$ $(x \in E)$.

Мы видим, таким образом, что задание пары (E, u), состоящей из конечномерного векторного пространства E и его эндоморфизма u, равносильно заданию модуля E_u (конечной размерности над K) (см. гл. II, § 7, n° 9). Так как $K[X]$ — *кольцо главных*

идеалов (гл. IV, § 1, предложение 7), то к модулю E_u можно применять результаты предыдущих параграфов.

Некоторые результаты этого параграфа обобщаются на случай, когда E — унитарный модуль над произвольным коммутативным кольцом (см. приложение).

Прежде чем применять эти результаты к модулю E_u, нам необходимо перевести некоторые понятия с языка модулей на язык эндоморфизмов векторных пространств:

«V — подмодуль в E_u» означает «V — векторное подпространство в E, устойчивое относительно u».

«V — моногенный подмодуль в E_u» означает «существует такой элемент $x \in V$, что векторное подпространство V порождается элементами $u^i x$ $(i \in \mathbf{N})$».

«$\mathfrak{a}$ — аннулятор подмодуля V» означает «$\mathfrak{a}$ — идеал, состоящий из таких многочленов $p(X) \in K[X]$, что $p(u)\,X = 0$ для любого $x \in V$».

Унитарный многочлен g, такой, что $\mathfrak{a}$ является главным идеалом (g), называется *минимальным многочленом* сужения эндоморфизма u на V.

«E_u — моногенный модуль, и аннулятор $\mathfrak{a} = (g)$»

$$(\text{где } g(X) = X^n + \alpha_{n-1}X^{n-1})$$

означает «существует такой элемент $x \in E$, что элементы $(u^i \cdot x)$ $(0 \leqslant i \leqslant n-1)$ составляют базис векторного пространства E, и $g(u) \cdot x = 0$». Другими словами, в пространстве E существует базис, относительно которого эндоморфизм u имеет матрицу

$$U = \begin{pmatrix} 0 & 0 & 0 \ldots 0 & -\alpha_0 \\ 1 & 0 & 0 \ldots 0 & -\alpha_1 \\ 0 & 1 & 0 \ldots 0 & -\alpha_2 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 \ldots 0 & -\alpha_{n-2} \\ 0 & 0 & 0 \ldots 1 & -\alpha_{n-1} \end{pmatrix}. \tag{2}$$

Имеет место, прежде всего, следующий результат:

Лемма 1. *Пусть E — векторное пространство конечной размерности n над полем K, и u — его эндоморфизм. $K[X]$-модуль E_u,*

определенный формулой (1), *является модулем кручения конечного типа.*

Пусть (e_i) $(1 \leqslant i \leqslant n)$ — базис пространства E; так как $K[X]$ содержит K, векторы e_i составляют систему образующих $K[X]$-модуля E_u, который является, таким образом, модулем конечного типа. С другой стороны, если бы он не был модулем кручения, то в нем имелся бы подмодуль, изоморфный $K[X]$; однако это невозможно, так как $K[X]$ имеет над K бесконечную размерность.

Теперь мы сформулируем в новых терминах теорему о разложении модуля кручения конечного типа, о котором идет речь в теореме 1 § 2, n° 2:

Предложение 1. *Пусть E — векторное пространство конечной размерности n над полем K, u — его эндоморфизм; для любого неприводимого унитарного многочлена $p(X)$, делящего минимальный многочлен $q(X)$ эндоморфизма u, через M_p обозначим векторное подпространство, состоящее из элементов $x \in E$, для которых существует такое целое число k, что $(p(u))^k x = 0$. Тогда M_p устойчиво относительно u, E — прямая сумма подпространств M_p и существуют такие многочлены s_p, что компонента любого элемента x в M_p равна $s_p(u)\,x$.*

Замечание. Ясно, что минимальный многочлен сужения эндоморфизма u на M_p является наибольшей степенью многочлена p, делящей q.

Аналогично по теореме 2 § 4 модуль E_u изоморфен прямой сумме моногенных модулей $F_j = K[X]/\mathfrak{a}_j$ $(1 \leqslant j \leqslant r)$, где $\mathfrak{a}_j$ — различные идеалы кольца $K[X]$ и $\mathfrak{a}_j \subset \mathfrak{a}_{j+1}$; этими условиями идеалы $\mathfrak{a}_j$ определяются однозначно. Так как, кроме того, E_u — модуль кручения, то $\mathfrak{a}_1 = (q) \neq (0)$; так как размерность E равна n, то $r \leqslant n$. Положим $\mathfrak{a}_i = (h_j)$ $(1 \leqslant j \leqslant r)$, где h_j — унитарный многочлен, и рассмотрим последовательность многочленов (q_i) $(1 \leqslant i \leqslant n)$, определяемую формулами

$$\begin{cases} q_i(X) = 1, & \text{если } i \leqslant n-r \\ q_i(X) = h_{n-i+1}(X), & \text{если } n-r < i \leqslant n. \end{cases} \tag{3}$$

Эта перемена обозначений имеет целью привести их в соответствие с обозначениями, применяемыми в приложении, где будет показано,

что модуль E_u канонически изоморфен некоторому фактормодулю свободного $K[X]$-модуля.

Ясно, что знание многочленов q_i эквивалентно знанию h_j, и модуль E изоморфен прямой сумме n модулей $K[X]/(q_i)$ $(1 \leqslant i \leqslant n)$, из которых первые $n - r$ сводятся к 0.

Другими словами:

Предложение 2. *Пусть E — векторное пространство конечной размерности над полем K, и u — его эндоморфизм. Существует n унитарных многочленов $q_i(X) \in K[X]$ $(1 \leqslant i \leqslant n)$ таких, что q_i делит q_{i+1} $(1 \leqslant i \leqslant n-1)$, и E является прямой суммой n подпространств V_i $(1 \leqslant i \leqslant n)$, устойчивых относительно u, моногенных (относительно u), а минимальный многочлен сужения эндоморфизма u на каждое V_i равен q_i $(1 \leqslant i \leqslant n)$. Многочлен q_i определяется этими условиями однозначно, и $q_n = q$ — минимальный многочлен эндоморфизма u.*

Замечание. Ввиду предыдущего предложения в пространстве E имеется базис, относительно которого матрица U эндоморфизма u принимает вид

$$\begin{pmatrix} A_{n-r+1} & 0 & \dots & 0 & 0 \\ 0 & A_{n-r+2} & \dots & 0 & 0 \\ 0 & 0 & \dots & A_{n-1} & 0 \\ 0 & 0 & \dots & 0 & A_n \end{pmatrix},$$

где каждая матрица A_i имеет вид (2) (при $g(X) = g_i(X)$).

Определение 1. *В обозначениях предложения 2, n унитарных многочленов $q_i(X)$ $(1 \leqslant i \leqslant n)$ называются инвариантами подобия эндоморфизма u (и всякой его матрицы U относительно произвольного базиса пространства E).*

Инвариант подобия q_n есть, таким образом, минимальный многочлен эндоморфизма u (предложение 2); иначе говоря, многочлен $p(X) \in K[X]$ удовлетворяет условию $p(u) = 0$ тогда и только тогда, когда p кратен q_n.

Обобщая терминологию, введенную для матриц (гл. II, § 6, n° 11), будем говорить, что эндоморфизм u унитарного A-модуля E и эндоморфизм u' унитарного A-модуля E' подобны, если существует такой изоморфизм g модуля E на E', что $u' \circ g = g \circ u$.

Следствие 1. *Для того чтобы эндоморфизмы u и u' конечномерных векторных пространств E и E' над одним и тем же полем K были подобны (соответственно матрицы U и U' эндоморфизмов u и u' относительно произвольных базисов в пространствах E и E' были подобны), необходимо и достаточно, чтобы они имели одинаковые инварианты подобия.*

В самом деле, утверждение, что u и u' имеют одинаковые инварианты подобия, равносильно тому, что модули E_u и E'_u изоморфны (§ 4, теорема 2); но из этого утверждения следует, что существует такой изоморфизм g векторного пространства E на векторное пространство E', что $u' \circ g = g \circ u$; обратно, такой изоморфизм g является также изоморфизмом модуля E_u на E'_u, так как для любого целого числа $n > 0$ выполняется равенство $u'^n \circ g = g \circ u^n$.

Следствие 2. *Пусть $q_i(X)$ $(1 \leqslant i \leqslant n)$ — инварианты подобия квадратной матрицы U порядка n с элементами из некоторого поля K; многочлены q_i остаются инвариантами подобия матрицы U, если рассматривать ее элементы как взятые из произвольного надполя K поля K.*

В самом деле, если многочлены $q_i \in K[X]$ таковы, что q_i делит q_{i+1} при $1 \leqslant i \leqslant n-1$, то утверждение, что они являются инвариантами подобия матрицы U (рассматриваемой как матрица с элементами из поля K), означает, что существует такая обратимая квадратная матрица P с элементами из поля K, что матрица $V = PUP^{-1}$ представляет собой квадратную таблицу из матриц вида (2), соответствующих многочленам q_i; поскольку элементы матрицы P и коэффициенты многочленов q_i принадлежат K', то следствие тем самым доказано.

Следствие 3. *Пусть U и V — квадратные матрицы порядка n с элементами из поля K. Если существует обратимая квадратная матрица P с элементами из некоторого надполя K поля K, такая, что $V = PUP^{-1}$, то существует обратимая квадратная матрица Q с элементами из поля Q, такая, что $V = QUQ^{-1}$.*

Это немедленно вытекает из следствий 1 и 2.

В Приложении мы дадим метод вычисления инвариантов подобия матрицы; из этого метода будет ясно, что они получаются из элементов матрицы с помощью рациональных действий.

Теперь сформулируем по-новому предложение 7 § 4 о разложении модуля в прямую сумму неразложимых подмодулей.

Предложение 3. *Пусть E — векторное пространство конечной размерности n над полем K, и u — его эндоморфизм. Тогда E является прямой суммой подпространств V_k, устойчивых относительно u и таких, что минимальный многочлен сужения u на V_k имеет вид $p_k^{n(k)}$, где p_k — неприводимый многочлен; кроме того, V_k не может быть разложено в прямую сумму двух подпространств, устойчивых относительно u, и не сводится к 0. Для любого неприводимого унитарного многочлена $p \in K[X]$ и любого целого числа $n \geqslant 1$ число $m(p^n)$ подпространств V_k из указанного разложения, таких, что p^n является минимальным многочленом сужения u на V_k, определяется однозначно.*

Знание многочленов $p_k^{n(k)}$ равносильно знанию инвариантов подобия эндоморфизма u: от одних к другим можно перейти способом, указанным в замечаниях 2 и 3 § 4, n° 7. Кроме того, от разложения, рассматриваемого в предложении 3, можно немедленно перейти к разложениям, рассмотренным в предложениях 2 и 3.

Заметим, что неприводимые унитарные многочлены $p \in K[X]$, такие, что $m(p^n) > 0$ при некотором целом $n \geqslant 1$, представляют собой не что иное, как неприводимые унитарные множители минимального многочлена эндоморфизма u. Следовательно, эти многочлены, в противоположность инвариантам подобия, зависят от поля K, в котором они рассматриваются.

2. Эндоморфизмы векторных пространств над алгебраически замкнутым полем

Предположим, что поле K алгебраически замкнуто; тогда всякий неприводимый унитарный многочлен над полем K имеет вид $X - \alpha$ ($\alpha \in K$) (гл. V, § 4, определение 1). Это позволяет высказать предложение 1 в следующей форме:

Предложение 4. *Пусть E — векторное пространство конечной размерности n над полем K, u — эндоморфизм пространства E и $q(X)$ — его минимальный многочлен. Для любого корня $\alpha \in K$ многочлена $q(X)$ через M_α обозначим векторное подпространство,*

состоящее из векторов $x \in E$, для которых существует целое число $k \geqslant 1$ такое, что $(u - \alpha)^k x = 0$. Тогда M_α устойчиво относительно u, E — прямая сумма подпространств M_α и существуют многочлены $s_\alpha \in K[X]$ такие, что компонента любого элемента $x \in E$ в M_α равна $s_\alpha(u)\, x$.

Подмодуль M_α является $K[X]$-модулем конечного типа, и поэтому его аннулятор имеет вид $(X - \alpha)^r$; другими словами, существует целое число $r \geqslant 1$ такое, что $(u - \alpha)^r x = 0$ для всех $x \in M_\alpha$; в этом случае говорят, что сужение на M_α эндоморфизма $u - \alpha$ является нильпотентным эндоморфизмом.

Замечание. Предположим, что в пространстве E существует базис $(e_j)_{1 \leqslant j \leqslant n}$, относительно которого эндоморфизм u имеет матрицу U с элементами из некоторого подполя K_0 поля K. Для любого K_0-автоморфизма σ поля K и любой точки $x = \sum_{j=1}^{n} \xi_j e_j$ пространства E положим $x^\sigma = \sum_{j=1}^{n} \xi_j^\sigma e_j$; отображение $x \to x^\sigma$ является, очевидно, взаимно однозначным полулинейным отображением E на себя; кроме того, предположение относительно матрицы U влечет равенство $u(x^\sigma) = (u(x))^\sigma$ для любого $x \in E$. Но коэффициенты минимального многочлена $q(X)$ эндоморфизма u лежат тогда в поле K_0 (следствие 2 предложения 2); следовательно, для любого корня α многочлена $q(X)$ и любого K_0-автоморфизма σ поля K α^σ также является корнем $q(X)$; кроме того, если $(u - \alpha)^k x = 0$, то и $(u - \alpha^\sigma)^k x^\sigma = 0$, и обратно; следовательно (в обозначениях предложения 3), $m(X - \alpha) = m(X - \alpha^\sigma)$ и $M_{\alpha\sigma} = (M_\alpha)^\sigma$. Кроме того, равенство $u(x^\sigma) = (u(x))^\sigma$ показывает, что если матрица сужения эндоморфизма u на M_α относительно некоторого базиса (a_k) подпространства M_α есть V_α, то V_α^σ будет матрицей сужения эндоморфизма u на $M_{\alpha\sigma}$ относительно базиса (a_k^σ).

По-прежнему предполагая, что поле K алгебраически замкнуто, применим к эндоморфизму u предложение 3. Многочлены p_k все имеют вид $X - \alpha$ (где α пробегает множество корней минимального многочлена q эндоморфизма u), и E является прямой суммой подпространств $E_{m,\alpha}$, устойчивых относительно u, моногенных (относительно u) и таких, что минимальный многочлен сужения эндоморфизма u на $E_{m,\alpha}$ равен $(X - \alpha)^m$. Пусть

$E'_{m,\alpha}$ — $K[X]$-модуль, ассоциированный с $E_{m,\alpha}$; тогда $E_{m,\alpha}$ изоморфен фактормодулю $K[X]/((X-\alpha)^m)$. Однако классы элементов $(X-\alpha)^k$ $(0 \leqslant k \leqslant m-1)$ по $\mathrm{mod}\,(X-\alpha)^m$ образуют базис модуля $K[X]/((X-\alpha)^m)$ относительно K (гл. IV, § 1, n° 5) и

$$X(X-\alpha)^k = \alpha(X-\alpha)^k + (X-\alpha)^{k+1}$$

при $0 \leqslant k \leqslant m-1$; отсюда следует, что пространство $E_{m,\alpha}$ имеет размерность m и в нем существует такой базис, относительно которого матрица сужения эндоморфизма u на $E_{m,\alpha}$ является матрицей порядка m и имеет вид

$$U_{m,\alpha} = \begin{pmatrix} \alpha & 0 & 0 & \dots & 0 & 0 \\ 1 & \alpha & 0 & \dots & 0 & 0 \\ 0 & 1 & \alpha & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \alpha & 0 \\ 0 & 0 & 0 & \dots & 1 & \alpha \end{pmatrix}. \tag{4}$$

Определение 2. *При любом целом $m \geqslant 1$ и любом $\alpha \in K$ матрица $U_{m,\alpha}$ называется жордановой матрицей порядка m, относящейся к числу α.*

Мы доказали, таким образом, следующее предложение:

Предложение 5. *Пусть U — квадратная матрица над алгебраически замкнутым полем K; существует матрица, подобная U и имеющая вид диагональной таблицы, состоящей из жордановых матриц.*

Заметив, что всякая жорданова матрица треугольна (гл. II, § 6, n° 5, пример 5), получаем:

Следствие. *Всякая квадратная матрица над алгебраически замкнутым полем подобна треугольной матрице.*

Замечания. 1) Заключение предложения 5 остается в силе, если вместо алгебраической замкнутости поля K предполагать лишь, что K содержит все корни минимального многочлена матрицы U.

2) Из предложения 3 следует, что если матрица U подобна диагональной таблице жордановых матриц (J_k), то число матриц J_k вида $U_{m,\alpha}$ (для фиксированных m и α) определяется однозначно матрицей U.

3) Заметив, что минимальный многочлен жордановой матрицы $U_{m,\alpha}$ равен $(X-\alpha)^m$, получаем следующий результат:

Предложение 6. *Если квадратная матрица U подобна диагональной таблице из жордановых матриц (U_{m_i,α_i}), то минимальный многочлен $q(X)$ матрицы U является н. о. к. многочленов $(X-\alpha_i)^{m_i}$; другими словами, $q(X)=\prod_{\alpha\in P}(X-\alpha)^{m_\alpha}$, где P — множество различных элементов семейства (α_i) и m_α — наибольший из показателей m_i, соответствующих индексам i, для которых $\alpha_i=\alpha$.*

4) Более общим образом, если матрица U подобна диагональной таблице из жордановых матриц $U_{m,\alpha}$, то методом, абсолютно аналогичным указанному в замечании 3 § 4, n° 7, легко вычисляются инварианты подобия матрицы U; надо выписать в одну строчку многочлены $(X-\alpha)^m$, относящиеся к одному и тому же α, расположив их в порядке убывания показателей степени, и дополнить их единицами; после этого инварианты подобия получаются, если брать произведения членов, стоящих в одном столбце. Например, для матрицы

$$\begin{pmatrix}2&0&0\\0&3&0\\0&1&3\end{pmatrix}$$

надо написать

$$(X-2),\ 1,\ 1$$
$$(X-3)^2,\ 1,\ 1,$$

и инварианты подобия будут равны $(X-2)(X-3)^2$, 1, 1.

3. Собственные значения и собственные векторы

Определение 3. *Пусть E — векторное пространство конечной размерности n над полем K, и — его эндоморфизм, U — матрица и относительно некоторого базиса (e_i) пространства E. Элемент $x\in E$ называется собственным вектором эндоморфизма и (и матрицы U), если существует такой элемент $\alpha\in K$, что $u\cdot x=\alpha x$; если $x\neq 0$, то скаляр α (вполне определяющийся элементом x) называется собственным значением эндоморфизма и (и матрицы U). Для любого собственного значения α эндоморфизма и множество V_α таких элементов $x\in E$, что $u\cdot x=\alpha x$, является векторным подпространством, устойчивым относительно и, и называется собственным подпространством E, относящимся к значению α.*

Пример. Для того чтобы вектор базиса e_i был собственным вектором матрицы $U = (u_{jk})$, необходимо и достаточно, чтобы $u_{ki} = 0$ для всех $k \neq i$; другими словами, столбец с номером i должен сводиться к своему диагональному члену; в этом случае собственный вектор e_i соответствует собственному значению $\alpha_i = u_{ii}$. Таким образом, для треугольной матрицы порядка n (например, для жордановой матрицы) вектор базиса, имеющий номер n, собственный; у диагональной матрицы все векторы базиса являются собственными, и это, очевидно, характеризует диагональные матрицы.

Замечание. Предположим, что в пространстве E имеется такой базис $(e_j)_{1 \leqslant j \leqslant k}$, что все элементы матрицы U эндоморфизма u относительно этого базиса принадлежат некоторому подполю K_0 поля K. В обозначениях замечания к предложению 4 ясно, что если α — собственное значение эндоморфизма u и $x \in E$ — соответствующий собственный вектор, то для любого K_0-автоморфизма σ поля K α^σ является собственным значением u, а x^σ — собственным вектором, соответствующим σ.

Утверждение, что $\alpha \in K$ является собственным значением эндоморфизма u (и матрицы U), означает, что ядро эндоморфизма $\alpha \cdot 1 - u$ содержит ненулевой вектор $x \in E$, то есть этот эндоморфизм необратим (гл. II, § 3, следствие предложения 11), и, кроме того, означает также, что выполняется равенство

$$\det(\alpha \cdot 1 - u) = \det(\alpha \cdot I_n - U) = 0.$$

Это приводит нас к следующему определению:

Определение 4. *Пусть U — квадратная матрица порядка n над полем K. Характеристическим многочленом матрицы U называется определитель $\chi_U(X)$ матрицы $X \cdot I_n - U$ (элементы этой матрицы лежат в $K[X]$):*

$$\chi_U(X) = \det(X \cdot I_n - U).$$

Из вычисления этого определителя сразу же следует, что характеристический многочлен матрицы U является унитарным многочленом степени n.

Пусть u — эндоморфизм векторного пространства E; отображение $X \cdot 1 - u$ является эндоморфизмом $K[X]$-модуля $E[X] = K[X] \otimes E$, получаемого из E расширением до $K[X]$ основного поля K (гл. III, § 2, n° 1). Если U — матрица эндоморфизма u относительно базиса (e_i) пространства E, то $X \cdot I_n - U$ — ма-

трица эндоморфизма $X \cdot 1 - u$ относительно (e_i), рассматриваемого как базис $K[X]$-модуля $E[X]$. Отсюда следует, что

$$\det(X \cdot 1 - u) = \det(X \cdot I_n - U);$$

это показывает, что $\det(X \cdot I_n - U)$ не зависит от выбора базиса (e_i), и позволяет назвать этот многочлен *характеристическим многочленом эндоморфизма* u. В терминах матриц это означает, что *характеристические многочлены двух подобных матриц совпадают*; впрочем, в этом легко убедиться прямым вычислением. Характеристический многочлен эндоморфизма u обозначается через $\chi_u(X)$.

Замечание перед определением 4 показывает, что:

Предложение 7. *Для того чтобы элемент $\alpha \in K$ был собственным значением эндоморфизма u, необходимо и достаточно, чтобы он был корнем характеристического многочлена эндоморфизма u.*

Предложение 8. *Пусть u — эндоморфизм некоторого векторного пространства конечной размерности n над полем K, $\chi_n(X)$ — его характеристический многочлен и $q_i(X)$ $(1 \leqslant i \leqslant n)$ — его инварианты подобия. Тогда*

$$\chi_u(X) = q_1(X)\, q_2(X) \ldots q_n(X).$$

Так как инварианты подобия не меняются при расширении основного поля (n° 1, следствие 2 предложения 2) и это справедливо, очевидно, и для характеристического многочлена, то можно считать, что поле K алгебраически замкнуто. Тогда существует (предложение 5) базис пространства E, относительно которого матрица эндоморфизма u является диагональной таблицей из жордановых матриц $U_{m(i),\,\alpha(i)}$ $(1 \leqslant i \leqslant q)$; тогда из вычисления инвариантов подобия (замечание 4 к предложению 5) следует, что произведение этих инвариантов равно $\prod_{i=1}^{q} (X - \alpha(i))^{m(i)}$.

Известно, с другой стороны, что определитель треугольной матрицы равен произведению ее диагональных элементов (гл. III, § 6, n° 4, пример 2); отсюда следует равенство $\det(X \cdot 1 - u) = \prod_{i=1}^{q} (X - \alpha(i))^{m(i)}$, что и доказывает предложение.

Следствие 1. *Пусть, в обозначениях предложения* 8, $q(X)$ — *минимальный многочлен эндоморфизма* u; *тогда* $q(X)$ *делит* $\chi_u(X)$ *и* $\chi_u(X)$ *делит* $q(X)^n$. *В частности, минимальный и характеристический многочлены эндоморфизма* u *имеют одинаковые корни в поле* K, *являющиеся собственными значениями* u.

Так как $q(X) = q_n(X)$, то очевидно, что $q(X)$ делит $\chi_u(X)$. С другой стороны, каждый многочлен q_i делит q, и следовательно, их произведение χ_u делит q^n.

Следствие 2 («теорема Гамильтона — Кэли»). *Для любого эндоморфизма и векторного пространства конечной размерности над полем выполняется равенство* $\chi_u(u) = 0$.

В самом деле, $\chi_u(X)$ является кратным минимального многочлена эндоморфизма u (следствие 1).

Следствие 3. *Для того чтобы эндоморфизм и был нильпотентен, необходимо и достаточно, чтобы его характеристический многочлен имел вид* X^n.

Это немедленно вытекает из следствия 1.

Следствие 4. *Предположим, что поле* K *алгебраически замкнуто, и для любого корня* α *многочлена* $\chi_u(X)$ *через* M_α *обозначим векторное подпространство в* E, *состоящее из тех элементов* $x \in E$, *для которых существует целое число* $k > 0$ *такое, что* $(u - \alpha)^k \cdot x = 0$ (см. предложение 4). *Если корень* α *имеет в* $\chi_u(X)$ *кратность* m, *то подпространство* M_α *имеет размерность* m.

Это немедленно следует из предложения 5 и вычисления определителя треугольной матрицы.

Замечания. 1) Пусть G — конечная абелева группа порядка m; легко проверить, что произведение инвариантных множителей группы G равно m. Таким образом, имеется аналогия между *характеристическим многочленом* матрицы и *порядком* конечной абелевой группы. Эта аналогия идет достаточно далеко; например, теорема Гамильтона — Кэли соответствует утверждению, что для любого элемента $x \in G$ выполняется равенство $mx = 0$. При этом, совершенно аналогично доказательству этого утверждения, можно легко провести прямое доказательство теоремы Гамильтона — Кэли (см. упражнение 1).

2) Теорема Гамильтона — Кэли обобщается на матрицы над произвольным коммутативным кольцом (см. n° 4, замечание 1 к предложению 10 и упражнение 18).

4. *Приведение к диагональному виду*

Определение 5. *Пусть E_k — векторное пространство конечной размерности n над полем K и u — его эндоморфизм. Говорят, что u приводится к диагональному виду, если в пространстве E имеется базис (e_i), относительно которого матрица эндоморфизма u диагональна.*

Это утверждение равносильно тому, что в пространстве E существует базис, состоящий из собственных векторов эндоморфизма u, или еще, что *собственные векторы эндоморфизма u порождают E.*

Предложение 9. *Пусть E — векторное пространство конечной размерности n над полем K, и u — его эндоморфизм, приводящийся к диагональному виду. Для любого собственного значения $\alpha \in K$ эндоморфизма u через V_α обозначим соответствующее собственное подпространство. Тогда E является прямой суммой V_α.*

Пусть (e_i) — базис пространства E, относительно которого эндоморфизм u имеет диагональную матрицу $U = (u_{ij})$, и пусть J_α, $\alpha \in K$,— множество таких индексов i, что $u_{ii} = \alpha$. Запишем условие принадлежности элемента $x = \sum_{i=1}^{n} \xi_i e_i$ $(\xi_i \in K)$ пространству V_α; оно означает, что $ux = \sum_{i=1}^{n} u_{ii}\xi_i e_i = \sum_{i=1}^{n} \alpha\xi_i e_i$, то есть $\xi_i = 0$ при $i \notin J_\alpha$. Таким образом, семейство $(e_i)_{i \in J_\alpha}$ является базисом в V_α, откуда непосредственно следует предложение.

Это предложение следует также из предложения 1 (n° 1).

Предложение 10. *Пусть E — векторное пространство конечной размерности n над полем K, и u — его эндоморфизм. Следующие утверждения эквивалентны:*

а) *Эндоморфизм u приводится к диагональному виду.*

б) *Все корни минимального многочлена $q(X)$ эндоморфизма u простые и лежат в K.*

В самом деле, каждое из условий а), б) означает, что в пространстве E имеется базис, относительно которого матрица U

эндоморфизма u имеет вид диагональной таблицы из жордановых матриц $U_{m,\alpha}$ (n° 2, определение 2). Вычисление минимального многочлена матрицы U (n° 2, предложение 6) показывает, что утверждения «все α — простые корни многочлена $q(X)$» и «все показатели m равны 1» эквивалентны. Однако последнее утверждение показывает, что U — диагональная таблица из матриц порядка 1, откуда и следует предложение.

Следствие. *Если все корни характеристического многочлена эндоморфизма и простые и лежат в K, то и приводится к диагональному виду.*

В самом деле, минимальный многочлен делит характеристический многочлен.

Замечания. 1) Если матрица U диагональна и (α_i) — ее диагональ, то матрица $X \cdot I_n - U$ диагональна, ее диагональ есть $(X - \alpha_i)$, и характеристический многочлен матрицы U равен $\prod_{i=1}^{n} (X - \alpha_i)$. Вычисление сумм и произведений диагональных матриц (гл. II, § 6, n° 5, упражнение 1) непосредственно показывает, что $\chi_U(U) = 0$. отсюда следует теорема Гамильтона — Кэли (следствие 2 предложения 8) для матриц, подобных некоторой диагональной матрице. Пусть теперь V_{ij} $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$ — n^2 переменных; рассмотрим матрицу $V = (V_{ij})$ с элементами из алгебраического замыкания Ω поля рациональных дробей $\mathbf{Q}((V_{ij}))$. Характеристический многочлен матрицы V является многочленом с *целыми* коэффициентами $P(V_{ij}, X)$ от переменных V_{ij} и X; характеристический многочлен произвольной матрицы (u_{ij}) над произвольным коммутативным кольцом равен $P(u_{ij}, X)$. Покажем, что все корни многочлена $P(V_{ij}, X)$, рассматриваемого как многочлен из кольца $\Omega[X]$, *простые*. В самом деле, пусть Z_k $(1 \leqslant k \leqslant n)$ — n переменных; рассмотрим многочлен $R(Z_k, X) = X^n + Z_1 X^{n-1} + \ldots + Z_n$ над полем $L = \mathbf{Q}(Z_1, \ldots, Z_n)$; пусть ζ_k $(1 \leqslant k \leqslant n)$ — его корни в алгебраическом замыкании поля L; элемент $\Delta = \prod_{i<j} (\zeta_i - \zeta_j)^2$ является *симметрическим* многочленом с целыми коэффициентами от переменных ζ_k, и следовательно, будет многочленом $\Phi(Z_1, Z_2, \ldots, Z_n)$ с целыми коэффициентами от Z_k (гл. V, Приложение I, предложение 3). Пусть $P(V_{ij}, X) = X^n + \sum_{k=1}^{n} F_k(V_{ij}) X^{n-k}$, где F_k — многочлены с целыми коэффициентами от V_{ij}; если бы многочлен P имел кратные корни, то выполнялось бы равенство $\Phi(F_1(V_{ij}), \ldots, F_n(V_{ij})) = 0$; но при подстановке сюда

вместо V_{ij} элементов некоторой диагональной матрицы с различными диагональными элементами получается противоречие. Следовательно, матрица V подобна диагональной матрице и $P(V_{ij}, V) = 0$. Так как элементы матрицы $P(V_{ij}, V)$ являются многочленами с *целыми* коэффициентами от переменных V_{ij}, то *принцип продолжения алгебраических тождеств* (гл. IV, § 2, схолия к теореме 3) показывает, что для любой матрицы $U = (u_{ij})$ над *произвольным коммутативным кольцом* выполняется равенство

$$\chi_U(U) = P(u_{ij}, U) = 0.$$

Это доказывает теорему Гамильтона — Кэли для общего случая матриц над коммутативным кольцом.

2) Заметим, что в предшествующем доказательстве мы не использовали других результатов, доказанных в этом параграфе: в самом деле, возможность приведения к диагональному виду матрицы, у которой все собственные значения различны, как у (V_{ij}), следует из того, что n соответствующих собственных векторов линейно независимы.

В процессе доказательства предложения 10 мы видели, что жорданова матрица может быть подобна диагональной матрице только в случае, если ее порядок равен 1. Заметим, что нильпотентный эндоморфизм, приводимый к диагональному виду, является нулевым.

Предложение 11. *Пусть E — векторное пространство конечной размерности n над алгебраически замкнутым полем K, u и — его эндоморфизм. Эндоморфизм u единственным способом можно представить в виде $u = v + w$, где v и w — перестановочные эндоморфизмы пространства E, v приводится к диагональному виду, а w нильпотентен. При этом v и w являются многочленами относительно u.*

Предположим, что существует пара (v, w), удовлетворяющая первой части утверждения; убедимся, что такая пара единственна. Пусть α — собственное значение *эндоморфизма* v и V_α — соответствующее собственное подпространство. Так как v и u перестановочны (поскольку $u = v + w$), то V_α устойчиво относительно u; это следует из леммы:

Лемма 2. *Пусть g и h — перестановочные эндоморфизмы векторного пространства E. Всякое собственное подпространство эндоморфизма g устойчиво относительно h.*

В самом деле, если W_λ — собственное подпространство эндоморфизма g, относящееся к собственному значению λ, то отношение $x \in W_\lambda$ влечет $.gh \cdot x = hg \cdot x = h \cdot \lambda x = \lambda h \cdot x$. Это показывает, что $hx \in W_\lambda$.

Следовательно, подпространство V_α устойчиво относительно u и w; так как сужение v на V_α является гомотетией с коэффициентом α, то сужение $u - \alpha$ на V_α совпадает с сужением на V_α эндоморфизма w и, следовательно, нильпотентно. Это означает, что V_α содержится в подпространстве M_α, состоящем из векторов $x \in E$, для которых существует такое целое число $k \geqslant 1$, что $(u - \alpha)^k x = 0$. Так как E является прямой суммой V_α (предложение 9) и прямой суммой M_α (предложение 4), то отсюда следует, что $V_\alpha = M_\alpha$. Следовательно, v однозначно определяется эндоморфизмом u: его сужение на каждое M_α является гомотетией с коэффициентом α.

Обратно, определим эндоморфизм v этим условием и положим $w = u - v$. Ясно, что v приводится к диагональному виду и эндоморфизм w нильпотентен. Остается убедиться в том, что u и w являются многочленами относительно u (отсюда уже будет следовать, что они перестановочны); достаточно показать это для v. Однако по предложению 4 существуют такие многочлены q_α, что компонента в M_α любого элемента $x \in E$ равна $q_\alpha(u)\, x$. Тогда $v = \sum_\alpha \alpha q_\alpha(u)$, что и заканчивает доказательство.

Замечания. 1) Пусть U — матрица эндоморфизма u; тогда $U = S + N$, где матрица S подобна диагональной матрице, N нильпотентна, и S и N являются многочленами относительно U. Если U является диагональной таблицей из жордановых матриц, то S сводится к ее диагонали, а N — треугольная матрица, состоящая из нулей и единиц (n° 2).

2) В общем случае можно сделать уточнение об элементах матриц S и N:

Предложение 12. *Пусть K — алгебраически замкнутое поле, F — его подполе, U — квадратная матрица, все элементы которой принадлежат F, и характеристический многочлен ее сепарабелен над F. Тогда все элементы матриц S и N принадлежат F.*

Пусть $L \subset K$ — поле корней характеристического многочлена матрицы U; существует такая обратимая квадратная матрица P

с элементами из поля L, что матрица PUP^{-1} является диагональной таблицей из жордановых матриц (замечание 1 к предложению 5); следовательно, все элементы матриц S и N принадлежат L. Пусть σ— произвольный F-автоморфизм поля K; для любого многочлена $p \in K[X]$ через p^σ обозначим многочлен, полученный из p после применения к его коэффициентам автоморфизма σ; аналогично для любой матрицы A над полем K через A^σ обозначим матрицу, полученную из A после применения к ее элементам автоморфизма σ; ясно, что если $B = p(A)$, то $B^\sigma = p^\sigma(A^\sigma)$.

Рассмотрим теперь матрицы S^σ и N^σ. Так как $U = U^\sigma$, то $U = S^\sigma + N^\sigma$; кроме того, матрица S^σ приводится к диагональному виду, N^σ нильпотентна, и если $S = p(U)$, то $S^\sigma = p^\sigma(U)$. Тогда из единственности разложения матрицы U следует, что $S^\sigma = S$ и $N^\sigma = N$; это означает, что элементы матриц S и N инвариантны при любом F-автоморфизме σ поля K. Однако, по предположению, поле L сепарабельно над F, и следовательно, элементы матриц S и N принадлежат F (гл. V, § 7, n° 2, определение 1).

Заметим, что заключение предложения 12 неверно, если характеристический многочлен матрицы U не сепарабелен над F (упражнение 12).

5. *Свойства характеристического многочлена; след и определитель*

Пусть E — векторное пространство конечной размерности n над полем K и u — его эндоморфизм. В § 3 мы определили *характеристический многочлен* эндоморфизма u, $\chi_u(X) = \det(X \cdot 1 - U)$. Напомним, что если эндоморфизм u имеет в базисе (e_i) пространства E матрицу U, то $\chi_u(X) = \chi_U(X) = \det(X \cdot I_n - U)$.

Свободный член этого многочлена равен $\chi_u(0) = (-1)^n \det(u)$. Найдем коэффициент при X^{n-1}; для этого положим $U = (u_{ij})$ и заметим, что при развертывании определителя

$$\det(X \cdot I_n - U) = \det(\delta_{ij} X - u_{ij})$$

члены, содержащие X^{n-1}, должны получиться по крайней мере из $n - 1$ диагональных множителей, и их в самом деле будет n. Следовательно, эти члены будут теми же, что у произведения

$\prod_{i=1}^{n}(X-u_{ii})$, так что искомый коэффициент равен $-\sum_{i=1}^{n}u_{ii}=-\operatorname{Tr}(u)$. Поэтому характеристический многочлен эндоморфизма u имеет вид

$$\chi_u(X)=X^n-\operatorname{Tr}(u)\,X^{n-1}+\ldots+(-1)^n\det(u). \tag{5}$$

Предложение 13. *Пусть E — векторное пространство конечной размерности n над алгебраически замкнутым полем K, и — эндоморфизм пространства E и $\chi_u(X)=\prod_{i=1}^{n}(X-\alpha_i)$ — разложение его характеристического многочлена на линейные множители. Для любого многочлена q с коэффициентами из K характеристический многочлен эндоморфизма $q(u)$ дается формулой*

$$\chi_{q(u)}(X)=\prod_{i=1}^{n}(X-q(\alpha_i)), \tag{6}$$

а его след и определитель — формулами

$$\operatorname{Tr}(q(u))=\sum_{i=1}^{n}q(\alpha_i) \tag{7}$$

и

$$\det(q(u))=\prod_{i=1}^{n}q(\alpha_i). \tag{8}$$

Ясно, что ввиду (5) формулы (7) и (8) следуют из (6). Для доказательства формулы (6) возьмем в пространстве E базис, относительно которого матрица $U=(u_{ij})$ эндоморфизма u *треугольна*, и применим следующую лемму:

Лемма 3. *Если B и C — треугольные матрицы порядка n и (β_i) и (γ_i) — их диагонали, то матрицы $B+C$ и BC треугольные, и их диагонали равны $(\beta_i+\gamma_i)$ и $(\beta_i\gamma_i)$.*

Это утверждение очевидно для суммы $B+C$. Если рассмотреть матрицы B и C как матрицы двух эндоморфизмов g и h относительно канонического базиса (e_i) пространства K^n, то предположение леммы означает, что $g(e_i)=\beta_i e_i+y_i$, $h(e_i)=\gamma_i e_i+z_i$, где векторы y_i и z_i принадлежат подпространству V_i, порожденному векторами e_k с индексами $k>i$. Так как V_i

устойчиво относительно g и h, то $g(h(e_i)) \equiv \beta_i \gamma_i e_i \pmod{V_i}$, что и доказывает утверждение для произведения BC.

Так как матрица U эндоморфизма u является треугольной матрицей с диагональю (α_i), то из леммы 3 по индукции следует, что $q(U)$ — треугольная матрица с диагональю $(q(\alpha_i))$. Тогда $XI_n - q(U)$ — треугольная матрица с диагональю $(X - q(\alpha_i))$, что и доказывает формулу (6).

Следствие 1. *Эндоморфизм и обратим тогда и только тогда, когда многочлен q независим с χ_u.*

В самом деле, утверждение, что многочлены q и χ_u независимы, равносильно утверждению, что они не имеют общих корней, то есть по формуле (8) $\det(q(u)) \neq 0$.

Замечание. Свойство быть независимым с χ_u равносильно свойству быть независимым с минимальным многочленом эндоморфизма u (следствие 1 к предложению 8). Поэтому предыдущее следствие вытекает также из предложения 1 § 1, n° 2.

Следствие 2. *Пусть $r \in K(X)$ — рациональная дробь над полем K. Для того чтобы эндоморфизм u допускал подстановку в r* (гл. IV, § 3, n° 2), *необходимо и достаточно, чтобы все его собственные значения α_i допускали подстановку в r. В этом случае выполняются формулы:*

$$\chi_{r(u)}(X) = \prod_{i=1}^{n} (X - r(\alpha_i)), \quad \operatorname{Tr}(r(u)) = \sum_{i=1}^{n} r(\alpha_i),$$

$$\det(r(u)) = \prod_{i=1}^{n} r(\alpha_i).$$

Запишем r в виде p/q, где p и q — независимые многочлены. Для того чтобы u допускал подстановку в r, необходимо и достаточно, чтобы $\det(q(u)) \neq 0$, откуда ввиду формулы (8) и следует первое утверждение. Поэтому ввиду следствия 1 нужно считать, что q независим с χ_u. Согласно тождеству Безу существуют многочлены g и h такие, что $qg + h\chi_u = 1$. Тогда имеем $q(\alpha_i)\, g(\alpha_i) = 1$, и ввиду теоремы Гамильтона — Кэли $q(u)\, g(u) = 1$. Теперь для получения нужных формул достаточно применить формулы (6), (7) и (8) к эндоморфизму $p(u)\, g(u) = r(u)$.

Следствие 3. *Для любого целого числа* $s \geqslant 0$ *выполняется равенство* $\mathrm{Tr}\,(u^s) = \sum_{i=1}^{n} \alpha_i^s$; *это равенство выполняется и для* $s < 0$, *если эндоморфизм и обратим.*

Это следствие является частным случаем предыдущего.

Следствие 4. *Пусть поле* K *имеет характеристику нуль; эндоморфизм* u *нильпотентен тогда и только тогда, когда* $\mathrm{Tr}\,(u^s) = 0$ *для* $1 \leqslant s \leqslant n$.

Если эндоморфизм u нильтотентен, то его собственные значения α_i равны нулю и $\mathrm{Tr}\,(u^s) = 0$ при любом $s > 0$ (следствие 3). Обратно, если $\mathrm{Tr}\,(u^s) = 0$ при $1 \leqslant s \leqslant n$, то все собственные значения α_i равны нулю, поскольку K имеет характеристику нуль (гл. V, приложение I, следствие предложения 4), и эндоморфизм u нильпотентен (предложение 4).

Следствие 5. *Матрица* $YI_n - U$ *обратима в кольце квадратных матриц над полем* $K(Y)$ *рациональных дробей над полем* K. *Кроме того,*

$$\mathrm{Tr}\,((YI_n - U)^{-1}) = \chi'_U(Y)/\chi_U(Y),$$

где χ'_U — *производная многочлена* χ_U.

В самом деле, взяв $r(X) = (Y - X)^{-1}$, можно рассмотреть $(Y \cdot I_n - U)^{-1}$ как рациональную дробь с коэффициентами из $K(Y)$. Тогда следствие немедленно вытекает из следствия 2 и формулы $\chi'_U(Y)/\chi_U(Y) = \sum_{i=1}^{n} (Y - \alpha_i)^{-1}$ (гл. V, приложение I, n° 3, формула (3)).

Замечание. Отметим, что следствия 1, 4 и 5 предложения 13 остаются в силе и в случае, если не предполагать поле K алгебраически замкнутым; в самом деле, достаточно выразить эти следствия в терминах матриц и рассмотреть элементы этих матриц как принадлежащие алгебраически замкнутому расширению поля K.

6. Характеристический многочлен тензорного произведения двух эндоморфизмов

Предложение 14. *Пусть* E (соответственно E') — *векторное пространство конечной размерности над алгебраически замкнутым полем* K, u (соответственно u') — *эндоморфизм пространства* E

(соответственно E') и $\chi_u(X) = \prod_i (X - \alpha_i)^{n_i}$ (соответственно $\chi_{u'}(X) = \prod_j (X - \beta_j)^{m_j}$) — *разложение его характеристического многочлена на линейные множители (все* α_i (соответственно β_j) *различны). Тогда характеристический многочлен эндоморфизма* $u \otimes u'$ *векторного пространства* $E \otimes E'$ *задается формулой*

$$\chi_{u\otimes u'}(X) = \prod_{i,j} (X - \alpha_i\beta_j)^{n_i m_j}.$$

Пусть V_i (соответственно V'_j) — подпространство в E (соответственно в E'), состоящее из элементов x, для которых существует такое целое число $k > 0$, что $(u - \alpha_i)^k = 0$ (соответственно $(u' - \beta_j)^k = 0$). Из следствия 4 к предложению 8 следует, что размерность V_i (соответственно V'_i) равна n_i (соответственно m_j). Так как E (соответственно E') — прямая сумма подпространств V_i (соответственно V'_j) (предложение 4), то $E \otimes E'$ — прямая сумма подпространств $V_i \otimes V'_j$ (гл. III, § 1, предложение 7). Однако сужение на $V_i \otimes V'_j$ эндоморфизма $u \otimes u' - \alpha_i\beta_j\,(e \otimes e')$, где e (соответственно e') — тождественный автоморфизм E (соответственно E'), нильпотентно; в этом можно убедиться, записав равенство $u \otimes u' - \alpha_i\beta_j\,(e \otimes e') = (u - \alpha_i e) \otimes u' + \alpha_i e \otimes (u' - \beta_j e')$ и заметив, что по формуле бинома сумма двух перестановочных нильпотентных элементов нильпотентна.

Так как размерность $V_i \otimes V'_j$ равна $n_i m_j$, то из следствия 3 к предложению 8 следует, что

$$\chi_{u\otimes u'}(X) = \prod_{i,j} (X - \alpha_i\beta_j)^{n_i m_j},$$

что и требовалось доказать.

7. *Применение: Нормальный базис циклического расширения*

Мы уже доказали (гл. V, § 10, n° 9, теорема 5), что всякое конечное расширение Галуа *бесконечного* поля K имеет *нормальный базис*. Теперь мы докажем эту теорему для случая, когда поле K произвольно (конечно или нет) и N — его циклическое расширение; этот результат применим к произвольному конечному рас-

ширению конечного поля K, так как всякое такое расширение циклично (гл. V, § 11, n° 4, предложение 5).

Пусть Γ — (циклическая) группа Галуа поля N, n — ее порядок, u — ее образующий. Автоморфизм u является эндоморфизмом поля N, рассматриваемого как векторное пространство размерности n над полем K. Пусть N_u — $K[X]$-модуль, ассоциированный с u (n° 1); для любого многочлена $p = \sum_{k=0}^{m} a_k X^k$ из кольца $K[X]$ произведение $p \cdot x$ $(x \in N_u)$ равно $\sum_{k=0}^{m} a_k u^k(x)$. Так как, по предположению, $u^n = 1$, то многочлен $X^n - 1$ кратен минимальному многочлену q эндоморфизма u (n° 1). Однако степень m многочлена q больше или равна n: в противоположном случае для любого $x \in N$ выполнялось бы равенство $\sum_{k=0}^{m} b_k u^k(x) = 0$ (где элементы $b_k \in K$ не все равны нулю), что противоречит *линейной независимости различных автоморфизмов* u^k $(0 \leqslant k \leqslant m < n)$ (гл. V, § 7, теорема 3). Следовательно, $X^n - 1$ является минимальным многочленом эндоморфизма u. Так как его степень равна n, он совпадает с характеристическим многочленом эндоморфизма u; остальные инварианты подобия эндоморфизма u равны 1 (предложение 8). Таким образом, модуль N_u изоморфен *моногенному* $K[X]$-модулю $K[X]/(X^n - 1)$ (предложение 2). Пусть $a \in N$ — образующий модуля N_u; тогда n элементов $u^k(a)$ $(0 \leqslant k \leqslant n-1)$ составляют систему образующих модуля N, рассматриваемого как векторное пространство над полем K, и линейно независимы над K, поскольку $[N : K] = n$; следовательно, они образуют *нормальный базис* расширения N.

Упражнения. 1) Пусть u — эндоморфизм векторного пространства E и V — подпространство в E, устойчивое относительно u. Показать, что характеристический многочлен сужения u на V делит характеристический многочлен эндоморфизма u. Вывести отсюда элементарное доказательство теоремы Гамильтона — Кэли (свести доказательство к случаю моногенного пространства и применить формулу (2)).

2) а) Показать, что всякая квадратная матрица над полем K подобна своей транспонированной матрице (свести доказательство к случаю жордановой матрицы).

б) Пусть u — эндоморфизм векторного пространства E конечной размерности над полем K. Всякое собственное значение λ эндоморфизма u является также собственным значением транспонированного эндоморфизма ${}^t u$ пространства E^*. Кроме того, пусть λ и μ — различные собственные значения эндоморфизма u, x — собственный вектор эндоморфизма u, соответствующий λ, x' — собственный вектор, соответствующий μ; показать, что x и x' ортогональны.

3) Пусть u — эндоморфизм векторного пространства E конечной размерности, λ — собственное значение эндоморфизма u, и v — эндоморфизм $u - \lambda$. Показать, что E является прямой суммой подпространств $v^{-1}(0)$ и $v(E)$ тогда и только тогда, когда λ — простой корень минимального многочлена эндоморфизма u.

4) Присоединяя к основному полю трансцендентный элемент, показать, что формула (6) в предложении 13 является следствием формулы (8). Доказать это утверждение непосредственно с помощью разложения многочлена q на линейные множители.

*5) а) Пусть K — алгебраически замкнутое поле, A — квадратная матрица порядка n над K, имеющая вид диагональной таблицы (A_i) из треугольных матриц, таких, что все собственные значения матрицы A_i равны одному и тому же элементу α_i $(1 \leqslant i \leqslant r)$, и $\alpha_i \neq \alpha_j$ при $i \neq j$. Показать, что всякая матрица B, перестановочная с A, является диагональной таблицей из матриц (B_i), где B имеет тот же порядок, что и A_i $(1 \leqslant i \leqslant r)$.

б) Пусть M — некоторое множество попарно перестановочных матриц порядка n над полем K. Показать, что, применяя ко всем матрицам из M одно и то же подобие, можно получить, что все они будут иметь вид диагональных таблиц из треугольных матриц (X_i), причем число r и порядки m_i матриц X_i одинаковы для всех матриц из M и все собственные значения матрицы X_i равны между собой (используя а), свести доказательство к случаю $r = 1$, затем применить лемму 2 для доказательства того, что в этом случае все матрицы из множества M имеют общий ненулевой собственный вектор, и в заключение провести индукцию по n).

6) Провести доказательство предложения 14 с помощью приведения матрицы к треугольному виду.

7) Пусть A — матрица из m строк и n столбцов ранга r над полем K, P — квадратная матрица порядка m, Q — квадратная матрица порядка n и $PAQ = A$. Показать, что существуют матрица P', подобная P, и матрица Q', подобная Q, такие, что

$$P' = \begin{pmatrix} R & S \\ 0 & U \end{pmatrix}, \qquad Q' = \begin{pmatrix} R^{-1} & 0 \\ S' & U' \end{pmatrix},$$

где R — обратимая квадратная матрица порядка r, U (соответственно U') — квадратная матрица порядка $m - r$ (соответственно $n - r$),

S (соответственно S') — матрица из r строк и m — r столбцов (соответственно из n — r строк и r столбцов).

8) Пусть E — векторное пространство конечной размерности n над полем K, u — его эндоморфизм, V — подпространство в E, устойчивое относительно u, и u_V — сужение эндоморфизма u на V. Показать, что если f_i $(1 \leqslant i \leqslant n)$ (соответственно g_i $(1 \leqslant j \leqslant m)$) — инварианты подобия эндоморфизма u (соответственно u_V), то при $1 \leqslant j \leqslant m$ многочлен g_j делит f_{j+n-m} (см. § 4, упражнение 8г)). Сформулировать и доказать аналогичное свойство для эндоморфизма пространства E/V, получаемого из u путем факторизации.

*9) Пусть A — квадратная матрица порядка n, B — квадратная матрица порядка m, C — матрица из m строк и n столбцов над полем K. Свести решение уравнения $XA = BX + C$, где X — неизвестная матрица из m строк и n столбцов над полем K, к решению системы линейных сравнений в кольце многочленов $K[Y]$. (Заметить, что для любого $f \in K[Y]$ должно выполняться равенство $Xf(A) = f(B)X + H(f)$, где $H(f)$ — однозначно определенная матрица из m строк и n столбцов; пусть $\sum_i E_i$ — разложение модуля E, ассоциированного с A (n° 1), в прямую сумму моногенных модулей и a_i — образующий модуля E_i; при этом аннуляторы модулей E_i являются отличными от 1 инвариантами подобия f_i матрицы A (предложение 2); аналогично определим подмодули F_j с образующими b_j и многочлены g_j для матрицы B; записать равенство $Xf_i(A)\,a_i = 0$; затем разложить Xa_i и $H(f_i)\,a_i$ на модули F_j и показать, что условия, получаемые таким образом из уравнений $Xf_i(A)\,a_i = 0$, необходимы и достаточны для существования решения.)

10) а) Показать, что матрица

$$\begin{pmatrix} \lambda & \alpha & \beta_{13} & \beta_{14} & \dots & \beta_{1n} \\ 0 & \lambda & \alpha & \beta_{24} & \dots & \beta_{2n} \\ 0 & 0 & \lambda & \alpha & \dots & \beta_{3n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & \alpha \\ 0 & 0 & 0 & 0 & \dots & \lambda \end{pmatrix}$$

над произвольным полем при $\alpha \neq 0$ подобна жордановой матрице $U_{n,\lambda}$.

б) Показать, что если $\lambda \neq 0$ и характеристика поля K равна 0, то для любого целого числа m (положительного или отрицательного) матрица $(U_{n,\lambda})^m$ подобна жордановой матрице U_{n,λ^m}.

в) Выполняется равенство $(U_{n,0})^m = 0$ для $m \geqslant n$. Если $0 < m < n$, то пусть $n - 1 = km + q$, где $0 \leqslant q < m$; показать, что $q + 1$ инвариантов подобия матрицы $(U_{n,0})$ равны X^{k+1}, а $m - q - 1$ инвариантов подобия равны X^k (расположить в подходящем порядке элементы канонического базиса пространства K^n).

г) Аналогичным образом определить инварианты подобия матрицы $f(U_n, \lambda)$, где $f \in K[X]$.

д) Исследовать те же вопросы для поля K характеристики $p \neq 0$.

11) Пусть K — алгебраически замкнутое поле, A — обратимая матрица над K, $m > 0$ — целое число. Показать, что если m не кратно характеристике поля K, то существует такой многочлен $g(X) \in K[X]$, что $(g(A))^m = A$ (использовать теорему Гамильтона — Кэли и упражнение 28 § 1). Обобщить это утверждение на уравнение $f(U) = A$ ($f \in K[X]$, U — неизвестная матрица порядка n над K).

12) а) Пусть u — эндоморфизм векторного пространства конечной размерности n над полем K. Показать, что если его характеристический многочлен неприводим и сепарабелен над K, то u приводится к диагональному виду над алгебраическим замыканием $\overline{K}$ поля K.

б) Показать, что если квадратная матрица над полем K имеет (в $\overline{K}$) собственное значение, не сепарабельное над K, то она не подобна (над K) никакой матрице, приводимой к диагональному виду (над $\overline{K}$) (использовать предложение 10).

в) Получить из б) пример матрицы, для которой неверно заключение предложения 12.

13) Пусть (λ_h) — конечное семейство различных ненулевых элементов поля K произвольной характеристики p. Показать, что если целые числа n_h удовлетворяют условию $\sum_h n_h \lambda_h^r = 0$ для достаточно большого r, то все n_h кратны p. (Заметить, что для любого целого числа s существует многочлен $f_h \in K[X]$ такой, что $f_h(\lambda_h) = 1$, $f_h(\lambda_k) = 0$ при $k \neq h$ и X^s делит f_h; для достаточно большого s из сделанного предположения следует, что $\sum_h n_h f_h(\lambda_h) = n_h \cdot 1 = 0$.)

Вывести отсюда, что если U — квадратная матрица порядка n над полем K характеристики 0, (λ_i) $(1 \leqslant i \leqslant n)$ — семейство элементов некоторого расширения поля K и для достаточно большого r выполняется равенство $\mathrm{Tr}(U^r) = \sum_{i=1}^{n} \lambda_i^r$, то $\chi_U = \prod_{i=1}^{n} (X - \lambda_i)$.

Отсюда и из упражнения 4 гл. III, § 4, прямым методом вывести результат предложения 14 для поля характеристики 0. Затем с помощью принципа сохранения алгебраических тождеств обобщить этот результат на поля произвольной характеристики.

*14) Пусть (Z_{ij}) $(1 \leqslant i, j \leqslant n)$ — семейство n^2 переменных над полем K_0, A — кольцо многочленов $K_0[Z_{11}, \ldots, Z_{nn}]$ и $K = K_0(Z_{ij})$ — его поле дробей; пусть χ_U — характеристический многочлен матрицы $U = (Z_{ij})$ над полем K.

а) Показать, что многочлен χ_U неприводим и сепарабелен. (Показать, что если χ_U приводим над K, то он является произведением двух многочленов от X степени > 0 из кольца $K_0[X, Z_{ij}]$; из этого вывести, что характеристический многочлен всякой квадратной матри-

цы порядка n над полем K приводим; получить противоречие с наличием примера многочлена, коэффициенты которого алгебраически независимы над K_0; аналогично рассмотреть сепарабельность.)

б) Показать, что матрица U подобна матрице, у которой все элементы равны 0, 1 или некоторому коэффициенту многочлена χ_U (см. n° 1, формула (2)). Вывести отсюда, что если поле K_0 бесконечно и p — многочлен из кольца A такой, что $p(u'_{ij}) = p(u''_{ij})$ всякий раз, когда матрицы (u'_{ij}) и (u''_{ij}) подобны над K_0, то p лежит в подкольце, порожденном в A коэффициентами многочлена χ_U. Сформулировать и доказать аналогичное утверждение для рациональных дробей $r \in K = K_0(Z_{ij})$.

15) Пусть E — левое векторное пространство конечной или бесконечной размерности над телом K, *не обязательно коммутативным*: пусть u — такой его эндоморфизм, что $u^2(x) = x$ для любого $x \in E$.

а) Показать, что если характеристика тела K не равна 2 и $v(x) = x + u(x)$, $w(x) = x - u(x)$, то E — прямая сумма подпространств $V = v(E)$ и $W = w(E)$, выполняются равенства $u(x) = x$ в V, $u(x) = -x$ в W. Вывести отсюда, что всякая квадратная матрица A порядка n над телом K, удовлетворяющая условию $A^2 = I_n$, подобна некоторой матрице вида

$$\begin{pmatrix} I_p & 0 \\ 0 & I_{n-p} \end{pmatrix}.$$

б) Если характеристика тела K равна 2 и $v(x) = x + u(x)$, то $v(E) \subset v^{-1}(0)$, и обратно. В частности, если эндоморфизм v имеет ранг p, то $2p \leqslant n$. Всякая квадратная матрица порядка n над телом K, удовлетворяющая условию $A^2 = I_n$, подобна некоторой диагональной таблице из $p + 1$ матриц $(I_{n-2p}, J, J, \ldots, J)$, где J — матрица

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

*16) Пусть K — алгебраически замкнутое поле, A — квадратная матрица порядка n над K.

а) Показать, что если $A = BC$, где $B^2 = C^2 = I$, то A обратима и подобна A^{-1}.

б) Пусть матрица A подобна жордановой матрице $U_{n,1}$ (n° 2). Показать, что если $A = BC$, где $B^2 = C^2 = I$, и u, v, w — эндоморфизмы пространства $E = K^n$, соответствующие матрицам A, B, C, то v и w имеют единственный (с точностью до гомотетии) общий собственный вектор, являющийся единственным (с точностью до гомотетии) собственным вектором эндоморфизма u.

в) В предположениях упражнения б) будем считать, что характеристика поля K не равна 2; показать, что B и C подобны. Пусть V^+, V^- (соответственно W^+, W^-) — подпространства в E, в которых $v(x) = x$ и $v(x) = -x$ соответственно (соответственно $w(x) = x$ и $w(x) = -x$); показать, что, заменяя при необходимости B и C на $-B$ и $-C$, можно

считать, что V^+ и W^+ имеют размерность $n/2$ при n четном и $\left[\frac{n}{2}\right]+1$ при n нечетном; кроме того, размерность $V^+ \cap W^+$ равна 1, а $V^- \cap W^-$ сводится к 0.

г) В предположениях упражнения б) будем считать, что поле K имеет характеристику 2. Пусть V (соответственно W) — подпространство в E, в котором $v(x) = x$ (соответственно $w(x) = x$); показать, что V и W оба имеют размерность $\left[\frac{n}{2}\right] + 1$ при n нечетном, а при n четном одно из них имеет размерность $n/2$, другое $\frac{n}{2}+1$ и в обоих случаях $V + W = E$.

д) Вывести из в) и г), что матрица $U_{n,1}$ является произведением BC, где $B^2 = C^2 = I$ (применить индукцию по n).

е) Показать, что всякая обратимая матрица A, подобная A^{-1}, является произведением BC, где $B^2 = C^2 = I$ (свести доказательство к случаю, когда A — таблица из жордановых матриц; использовать д), упражнение 10а) и следующее замечание: если $U = U_{n,1}$ и $\lambda \in K$ не равно 0, то существуют $\mu \in K$ и такие матрицы V и W, что $V^2 = W^2 = I$ и

$$\begin{pmatrix} \lambda U & 0 \\ 0 & \lambda^{-1}U^{-1} \end{pmatrix} = \begin{pmatrix} 0 & \mu V \\ \mu^{-1}V & 0 \end{pmatrix} \begin{pmatrix} 0 & \mu^{-1}W \\ \mu W & 0 \end{pmatrix}.$$

*17) Пусть K — алгебраически замкнутое поле характеристики $\neq 2$ и квадратные матрицы A_i $(1 \leqslant i \leqslant s)$ порядка n над K удовлетворяют соотношениям

$$A_i^2 = -(1 \leqslant i \leqslant s), \quad A_iA_j = -A_jA_i \qquad (i \neq j).$$

а) Показать, что при $s > 1$ для любого i, $1 \leqslant i \leqslant s$, выполняется равенство $\mathrm{Tr}(A_i) = 0$; вывести отсюда, что тогда n четно и что всякая матрица A_i имеет $n/2$ собственных значений, равных ω, и $n/2$ значений, равных $-\omega$ ($\omega^2 = -1$), и приводится к диагональному виду.

б) Показать, что существует подобие, приводящее матрицу A_1 к жордановой форме, а матрицы A_k $(k > 1)$ к виду

$$\begin{pmatrix} 0 & B_k \\ -B_k^{-1} & 0 \end{pmatrix},$$

где B — единичная матрица порядка $n/2$, и $s - 2$ матриц B_k $(k > 2)$ порядка $n/2$ удовлетворяют условиям

$$B_i^2 = -I\ (3 \leqslant i \leqslant s), \quad B_iB_j = -B_jB_i \qquad (i \neq j).$$

в) Вывести из б), что если $n = 2^q r$, где r нечетно, то $s \leqslant 2q + 1$ и найдется $r + 1$ систем из $2q + 1$ матриц, не переводящихся одна в другую подобием и обладающих рассматриваемыми свойствами.

*18) а) Пусть A — коммутативное кольцо с единицей, B — коммутативная алгебра над A с базисом (e_i) (конечным или нет),

и пусть $e_ie_j = \sum_h c_{ijh}e_h$ — таблица умножения в этом базисе. Пусть $U = \sum_i U_ie_i$ — квадратная матрица порядка n над B, где U_i — квадратные матрицы порядка n над A, все, кроме конечного числа, равные нулю. Можно написать равенство $\det(U) = \sum_i \lambda_i e_i$, где $\lambda_i \in A$ ($\lambda_i = 0$ для всех индексов, кроме конечного числа). Показать, что если матрицы X_i над A попарно перестановочны и обладают свойствами

$$X_iX_j = \sum_h c_{ijh}X_h \quad \text{и} \quad \sum_i U_iX_i = 0, \quad \text{то} \quad \sum_i \lambda_iX_i = 0$$

(использовать тождество $U'U = (\det U)\,I$, где U' — присоединенная матрица). Вывести отсюда, в частности, что если X — квадратная матрица над A, то многочлен $\chi_X(Z) = \det(ZI_n - X)$ удовлетворяет соотношению Гамильтона — Кэли $\chi_X(X) = 0$.

б) Пусть X — квадратная матрица порядка n над A и $(h_{ij}(Z))$ — присоединенная матрица к $Z \cdot I_n - X$; показать, что многочлен $g(Z) \in A[Z]$ обладает свойством $g(X) = 0$ тогда и только тогда, когда при любых i и j произведение $g(Z)\,h_{ij}(Z)$ кратно $\chi_X(Z)$ (заметить, что при любом $g \in A[Z]$ можно написать равенство $g(Z) \cdot I_n - g(X) = (Z \cdot I_n - X)\,Y$, где Y — матрица над кольцом $A[Z]$).

19) Пусть A — коммутативное кольцо с единицей, X и Y — квадратные матрицы порядка n над A; показать, что характеристические многочлены матриц XY и YX равны (сначала доказать это утверждение для случая, когда A — поле и матрица X обратима, а затем применить принцип продолжения алгебраических тождеств). Привести пример, в котором A — поле и матрицы XY и YX имеют разные ранги и, следовательно, не подобны.

*20) а) Пусть K — тело, *коммутативное или нет*. Рассмотрим векторное пространство E размерности n над K и эндоморфизм u этого пространства такой, что $B_1 = u^{-1}(0)$ не сводится к 0; пусть u_s — s-я итерация эндоморфизма u, $B_s = u_s^{-1}(0)$ и r — наименьшее число, для которого $u_{r+1}(E) = u_r(E)$; показать, что r является также наименьшим числом, таким, что $B_r = B_{r+1}$, и E является прямой суммой B_r и $u_r(E)$; показать также, что сужение u на $u_r(E)$ — эндоморфизм.

б) Будем предполагать теперь, что $B_r = E$; положим $h_s = \dim B_s - \dim B_{s-1}$, где $B_0 = \{0\}$ ($1 \leqslant s \leqslant r$). Показать, что пространство E является прямой суммой r подпространств F_s ($1 \leqslant s \leqslant r$), где F_s — прямая сумма h_s подпространств $G_{\alpha,s}$ размерности s, инвариантных относительно u, и при подходящем выборе базиса в E сужение эндоморфизма u на $G_{\alpha,s}$ имеет жорданову матрицу. Получить отсюда новое изложение теории приведения к жордановой форме квадратных матриц над алгебраически замкнутым полем.

*21) а) Пусть A — квадратная матрица порядка n над алгебраически замкнутым полем и $\chi_A(X) = \prod_{i=1}^{n}(X - \alpha_i)$ — разложение ее характеристического многочлена на множители первой степени. Показать, что при $1 \leqslant p \leqslant n$ характеристический многочлен p-й внешней степени матрицы A (гл. III, § 6, n° 3) равен $\prod_H (X - \alpha_H)$, где H пробегает множество последовательностей из p целых чисел $(i_k)_{1 \leqslant k \leqslant p}$ таких, что $1 \leqslant i_1 < i_2 < \ldots < i_p \leqslant n$, и для всякой такой последовательности $H = (i_k)$ положено $\alpha_H = \alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_p}$. Вывести отсюда, что $\det(\bigwedge^p A) = (\det A)^{\binom{n}{p-1}}$.

б) Пусть A — жорданова матрица $U_{n,\alpha}$, $\alpha \neq 0$. Показать, что при $n \geqslant 3$ p-я внешняя степень матрицы A подобна диагональной таблице из жордановых матриц U_{r,α^p}, где $3 \leqslant r \leqslant n$, и число c_{npr} этих матриц, имеющих порядок r, удовлетворяет следующим соотношениям: $c_{n1r} = 0$ при $r > n$, $c_{np1} = 1$ при $p = 1$ и $p = n - 1$, $c_{npn} = 0$ при $1 < p < n - 1$, и, наконец, $c_{n+1,\,p,r} = c_{npr} + c_{n,\,p-1,\,r}$ (расположить индексы H в лексикографическом порядке и воспользоваться упражнением 10а)).

22) Пусть T_{ij} $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$ — n^2 переменных и $T = (T_{ij})$ — матрица порядка n над кольцом $\boldsymbol{Z}[T_{11}, \ldots, T_{nn}]$. Обозначим через $\Delta(T_{11}, \ldots, T_{nn})$ (соответственно $\Delta^{ij}(T_{11}, \ldots, T_{nn})$) определитель матрицы T (соответственно алгебраическое дополнение в T элемента T_{ij}); эти выражения являются многочленами от T_{ij} с целыми коэффициентами.

Пусть X_{ij} $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$ — n^2 *попарно перестановочных* квадратных матриц порядка p над коммутативным кольцом A с единицей и U — квадратная матрица порядка np над A, имеющая вид квадратной таблицы из матриц

$$U = \begin{pmatrix} X_{11}X_{12} \ldots X_{1n} \\ X_{21}X_{22} \ldots X_{2n} \\ \ldots\ldots\ldots \\ X_{n1}X_{n2} \ldots X_{nn} \end{pmatrix}.$$

Показать, что определитель матрицы U равен определителю квадратной матрицы $\Delta(X_{11}, \ldots, X_{nn})$ порядка p. Провести индукцию по n, рассматривая два случая:

а) Положим $Y_{ij} = \Delta^{ij}(X_{11}, \ldots, X_{nn})$ и предположим сначала, что $\det Y_{11}$ не является в A делителем 0; умножить тогда матрицу U слева на

$$\begin{pmatrix} Y_{11} & Y_{21} \ldots Y_{n1} \\ 0 & I_p \ldots 0 \\ \ldots\ldots\ldots \\ 0 & 0 \ldots I_p \end{pmatrix}.$$

б) Общий случай свести к а), рассматривая матрицу $Z \cdot I_{np} - U$ над кольцом многочлена $A[Z]$ от одного переменного Z.

23) Пусть A — коммутативное кольцо с единицей, X_{ij} $(1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n)$ — n^2 *попарно перестановочных* квадратных матриц порядка n над кольцом A, $(e_i)_{1 \leqslant i \leqslant n}$ — базис A-модуля A^n. Предположим, что выполняются n соотношений $\sum_{j=1}^{n} X_{ijej} = 0$ $(1 \leqslant i \leqslant n)$, где e_i отождествлен с матрицей-столбцом из своих компонент относительно канонического базиса модуля A^n. Показать, что (в обозначениях упражнения 22) $\Delta(X_{11}, \ldots, X_{nn}) = 0$. (Положив в этих обозначениях $Y_{ij} = \Delta^{ij}(X_{11}, \ldots, X_{nn})$, рассмотреть уравнения $\sum_{i=1}^{n} Y_{ik} (\sum_{j=1}^{n} X_{ijej}) = 0$.)

Получить из этого результата новое доказательство теоремы Гамильтона — Кэли (если $X = (\alpha_{ij})$, то $\sum_{j=1}^{n} (\alpha_{ij} I - \delta_{ij} X) e_j = 0$, где δ_{ij} — символ Кронекера и (e_i) — канонический базис модуля A^n).

ПРИЛОЖЕНИЕ

ЭНДОМОРФИЗМЫ УНИТАРНЫХ МОДУЛЕЙ

Обобщим некоторые результаты § 5 на эндоморфизмы произвольных унитарных модулей над коммутативным кольцом. В дальнейшем A — *коммутативное* кольцо с единицей (и, быть может, с делителями нуля), E — унитарный A-модуль и u — эндоморфизм модуля E.

1. *Модуль, ассоциированный с эндоморфизмом*

Рассмотрим кольцо многочленов $A[X]$ от одного переменного X над кольцом A. Для любого многочлена $p \in A[X]$ и любого $x \in E$ положим

$$px = p(u)\,x; \tag{1}$$

тем самым определено билинейное отображение $(p, x) \to px$ произведения $A[X] \times E$ в E, задающее на E структуру *унитарного* $A[X]$-*модуля*. Множество E, наделенное этой структурой, обозначается E_u; заданная на E структура A-модуля получается сужением на A кольца операторов модуля E_u. Заметим, что подмодули модуля E_u представляют собой не что иное, как подмодули модуля A, устойчивые относительно u.

Так как отображение $(p, x) \to px$ произведения $A[X] \times E$ в E A-билинейно, то оно канонически определяет A-линейное отображение φ тензорного произведения $A[X] \otimes E$ A-модулей $A[X]$ и E в A-модуль E: для любых $p \in A[X]$ и $x \in E$ имеем

$$\varphi(p \otimes x) = p \cdot x = p(u) \cdot x \tag{2}$$

(гл. III, § 1).

С другой стороны, известно (гл. III, § 2), что тензорное произведение $A[X] \otimes E$ наделяется структурой $A[X]$-*модуля*

с помощью равенства $q\,(p \otimes x) = (qp) \otimes x$ для любого $q \in A\,[X]$; выполняется равенство

$$\varphi\,(q\,(p \otimes x)) = \varphi\,((qp) \otimes x) = (qp) \cdot x = q\,(u)\,(p\,(u)\,x) = q \cdot \varphi\,(p \otimes x),$$

и поэтому φ является, в смысле этой структуры, $A\,[X]$-линейным отображением $A\,[X]$-модуля $A\,[X] \otimes E$ в $A\,[X]$-модуль E_u.

Мы предполагаем изучить структуру $A\,[X]$-модуля E_u с помощью отображения φ. Заметим, что u является $A\,[X]$-эндоморфизмом модуля E_u, так как $u\,(px) = (up\,(u))\,x = p\,(ux)$. С другой стороны, формула

$$\bar{u}\,(p \otimes x) = p \otimes (ux) \tag{3}$$

определяет $A\,[X]$-эндоморфизм $\bar{u}$ тензорного произведения $A\,[X] \otimes E$.

Из формул (2) и (3) сразу же следует, что $A\,[X]$-линейные отображения u, $\bar{u}$ и φ связаны соотношением

$$\varphi \circ \bar{u} = u \circ \varphi. \tag{4}$$

Наконец, обозначим через ψ $A\,[X]$-эндоморфизм $X - \bar{u}$ тензорного произведения $A\,[X] \otimes E$ (другими словами, $\psi\,(p \otimes x) = (Xp) \otimes x - p \otimes (u \cdot x)$). Тогда имеем следующее предложение:

Предложение 1. *Образ тензорного произведения* $A\,[X] \otimes E$ *при* $A\,[X]$*-линейном отображении* φ *равен* E_u; *ядро* $\bar{\varphi}^{-1}(0)$ *отображения* φ *совпадает с образом* $A\,[X] \otimes E$ *при эндоморфизме* $\psi = X - \bar{u}$.

Так как $\varphi\,(1 \otimes x) = x$ для любого $x \in E$, то, очевидно, φ является отображением $A\,[X] \otimes E$ *на* E; с другой стороны,

$$\varphi\,(X\,(p \otimes x)) = X \cdot \varphi\,(p \otimes x) = u \cdot \varphi\,(p \otimes x);$$

иными словами, $\varphi \circ X = u \circ \varphi$; ввиду (4) $\varphi \circ \psi = 0$, то есть образ M тензорного произведения $A\,[X] \otimes E$ при отображении ψ содержится в $\bar{\varphi}^{-1}(0)$. Таким образом, достаточно доказать, что $\bar{\varphi}^{-1}(0) \subset M$.

Для этого заметим, что поскольку одночлены X^k $(k \geqslant 0)$ образуют базис A-модуля $A\,[X]$, то всякий элемент $z \in A\,[X] \otimes E$ однозначно записывается в виде $z = \sum\limits_k X^k \otimes x_k$, где элементы

$x_k \in E$ все, кроме конечного числа, равны нулю. Если $z \in \bar{\varphi}^{-1}(0)$, то $\varphi(z) = \sum_k u^k \cdot x_k = 0$, и можно написать

$$z = \sum_k (X^k \otimes x_k - 1 \otimes (u^k \cdot x_k)) = \sum_k (X^k - \bar{u}^k)(1 \otimes x_k).$$

Но $A[X]$-эндоморфизмы X и $\bar{u}$ тензорного произведения $A[X] \otimes E$ *перестановочны*, так что $X^k - \bar{u}^k$ является композицией $X - \bar{u}$ и $\sum_{j=0}^{k-1} X^j \bar{u}^{k-j-1}$; это доказывает существование элемента $y \in A[X] \otimes E$ такого, что $z = \psi y$.

Следствие. *$A[X]$-модуль E_u изоморфен фактормодулю $A[X]$-модуля $A[X] \otimes E$ по образу $A[X] \otimes E$ при эндоморфизме $\psi = X - \bar{u}$.*

2. *Подобные эндоморфизмы*

В этом n° E и E' — унитарные A-модули, u — эндоморфизм модуля E, u' — эндоморфизм модуля E'; обозначения E_u, φ, $\bar{u}$, ψ употребляются в том же смысле, что и в n° 1, а $E'_{u'}$, φ', $\bar{u}'$, ψ' означают аналогично определенные модуль и отображения, соответствующие E' и u'.

Предложение 2. *Для того чтобы отображение g модуля E в E' было $A[X]$-линейным отображением модуля E_u в $E'_{u'}$, необходимо и достаточно, чтобы g было A-линейным отображением модуля E в E' таким, что $g \circ u = u' \circ g$.*

Ввиду (1) это условие, очевидно, необходимо; но индукцией по n из него следует, что $g \circ u^n = u'^n \circ g$, так что оно и достаточно.

Следствие. *Для того чтобы отображение g было изоморфизмом модуля E_u на $E'_{u'}$, необходимо и достаточно, чтобы g было изоморфизмом E на E' таким, что $g \circ u = u' \circ g$, другими словами, чтобы u и u' были подобны.*

Пусть g — A-линейное отображение модуля E в E'; известно (гл. III, § 2), что отображение g канонически определяет $A[X]$-линейное отображение $\bar{g}$ тензорного произведения $A[X] \otimes E$

в $A[X] \otimes E'$: для любых $p \in A[X]$ и $x \in E$

$$\bar{g}(p \otimes x) = p \otimes g(x). \tag{5}$$

Предложение 3. *Пусть g — $A[X]$-линейное отображение модуля E_u в $E'_{u'}$; тогда*

$$\varphi' \circ \bar{g} = g \circ \varphi \tag{6}$$

и

$$\psi' \circ \bar{g} = \bar{g} \circ \psi. \tag{7}$$

В самом деле, по предположению, если $p \in A[X]$ и $x \in E$, то $\varphi'(\bar{g}(p \otimes x)) = \varphi'(p \otimes g(x)) = p(u')\, g(x) = g(p(u))\, x) = g(\varphi(p \otimes x))$, что доказывает (6). Аналогично

$$\bar{u}'(\bar{g}(p \otimes x)) = \bar{u}'(p \otimes g(x)) = p \otimes (u' \cdot g(x)) = p \otimes g(u \cdot x) = \bar{g}(u(p \otimes x)),$$

что и доказывает (7).

Предложение 4. *Если существуют $A[X]$-линейные отображения g_1, g_2 модуля $A[X] \otimes E$ в $A[X] \otimes E'$ такие, что $\psi' \circ g_2 = g_1 \circ \psi$, то существует $A[X]$-линейное отображение g модуля E_u в $E'_{u'}$ такое, что $\varphi' \circ g_1 = \varphi' \circ \bar{g}$. Если, кроме того, g_1 и g_2 — $A[X]$-изоморфизмы модуля $A[X] \otimes E$ на $A[X] \otimes E'$, то g — $A[X]$-изоморфизм модуля E_u на $E'_{u'}$.*

В самом деле, пусть M (соответственно M') — образ модуля $A[X] \otimes E$ (соответственно $A[X] \otimes E'$) при отображении ψ (соответственно ψ'). Тогда из предположения следует, что $g_1(M) \subset M'$. Следовательно, отображение g_1 определяет путем факторизации $A[X]$-линейное отображение фактормодуля $(A[X] \otimes E)/M$ в фактормодуль $(A[X] \otimes E')/M'$; так как модули эти канонически изоморфны соответственно E_u и $E'_{u'}$, то, по предложению 3, тем самым получено $A[X]$-линейное отображение g модуля E_u в $E'_{u'}$ такое, что $\varphi'(g_1(p \otimes x)) = g(\varphi(p \otimes x))$, но вследствие (6) это соотношение означает, что $\varphi' \circ g_1 = \varphi' \circ \bar{g}$. Наконец, если g_1 и g_2 являются изоморфизмами, то $g_1(M) = M'$, и следовательно, g — изоморфизм модуля E_u на $E'_{u'}$.

Обобщая терминологию, введенную для матриц (гл. II, § 6, n° 10), будем говорить, что эндоморфизмы u и u' *эквивалентны*, если существуют такие изоморфизмы f_1 и f_2 модуля E на E', что $u' \circ f_2 = f_1 \circ u$. Предложение 4 влечет

Следствие. *Для того чтобы эндоморфизмы u и u' (соответственно A-модулей E и E') были подобны, необходимо и достаточно, чтобы эндоморфизмы $X - \overline{u}$ и $X - \overline{u'}$ ($A[X]$-модулей $A[X] \otimes E$ и $A[X] \otimes E'$ соответственно) были эквивалентны.*

Замечание. Из формулы (7) следует, что если u и u' подобны, то $X - \overline{u}$ и $X - \overline{u'}$ подобны; следовательно, для эквивалентности эндоморфизмов $X - \overline{u}$ и $X - \overline{u'}$ необходимо и достаточно, чтобы они были подобны. Разумеется, это совпадение основано на частном виде этих эндоморфизмов и не имеет места для произвольных эндоморфизмов модулей $A[X] \otimes E$ и $A[X] \otimes E'$.

3. *Применение к эндоморфизмам векторных пространств*

Пусть E — векторное пространство конечной размерности n над полем K, и u — его эндоморфизм. По предложению 2 $K[X]$-модуль E_u, ассоциированный с u, изоморфен фактормодулю $K[X]$-модуля $K[X] \otimes E$ по подмодулю M, образу $K[X] \otimes E$ при эндоморфизме $X - \overline{u}$. Однако если $(e_j)_{1 \leqslant j \leqslant n}$ — произвольный базис пространства E над K, то элементы $1 \otimes e_j$ $(1 \leqslant j \leqslant n)$ образуют базис модуля $K[X] \otimes E$ над $K[X]$; другими словами, $K[X] \otimes E$ — *свободный* $K[X]$-модуль конечного типа; отсюда следует, что инварианты подобия $q_i(X)$ эндоморфизма u (§ 5, определение 1, п° 1) представляют собой не что иное, как *инвариантные факторы* подмодуля M относительно $K[X]$-модуля $K[X] \otimes E$ (§ 4, п° 2, определение 1). Отсюда получается метод вычисления многочленов $q_i(X)$: по предложению 1 элементы $X \otimes e_j - 1 \otimes (u \cdot e_j)$ составляют систему образующих подмодуля M; но если U — матрица эндоморфизма u относительно (e_i), то координаты элемента $X \otimes e_j - 1 \otimes (ue_j)$ относительно базиса $(1 \otimes e_j)$ модуля $K[X] \otimes E$ представляют собой элементы столбца с номером j матрицы $XI_n - U$ (над $K[X]$). Тогда из предложения 3 § 4 следует

Предложение 5. *Пусть E — векторное пространство конечной размерности над полем K, и u — его эндоморфизм, U — матрица u относительно произвольного базиса пространства E. Для любого целого числа m, такого, что $1 \leqslant m \leqslant n$, произведение*

$$d_m(X) = q_1(X)\, q_2(X) \ldots q_m(X)$$

первых r инвариантов подобия эндоморфизма u равно н. о. д. миноров порядка r матрицы $X \cdot I_n - U$.

Тем самым, в частности, вновь получено предложение 8 § 5.

Упражнения. 1) а) С помощью следствия предложения 4 провести новое доказательство того, что квадратная матрица над полем подобна своей транспонированной.

б) Показать, что матрица $\begin{pmatrix} 4 & 1 \\ 0 & 1 \end{pmatrix}$ над кольцом $\boldsymbol{Z}$ целых рациональных чисел не подобна своей транспонированной.

2) Пусть E — унитарный модуль над коммутативным кольцом A, имеющий конечный базис $(e_j)_{1 \leqslant j \leqslant n}$; отождествим каждый элемент e_j с элементом $1 \otimes e_j$ $A[X]$-модуля $A[X] \otimes E$; тогда базис (e_j) отождествится с базисом этого модуля. Дать новое доказательство теоремы Гамильтона — Кэли, доказав, что, в обозначениях предложения 1, $\chi_u(X)\, e_j \in M$ для любого индекса j; для этого заметить, что если (e'_j) — базис, сопряженный к (e_j), модуля, сопряженного к $A[X] \otimes E$, то

$$e_j = (-1)^{n-j} (e_1 \wedge \ldots \wedge e_n) \llcorner (e'_1 \wedge \ldots \wedge e'_{j-1} \wedge e'_{j+1} \wedge \ldots \wedge e'_n)$$

и, с другой стороны,

$$\chi_u(X)\,(e_1 \wedge e_2 \wedge \ldots \wedge e_n) = (Xe_1 - \bar{u}(e_1)) \wedge \ldots \wedge (Xe_n - \bar{u}(e_n)).$$

Наконец, использовать упражнение 2 § 8 гл. III.

3) Говорят, что пары (A_1, A_2) и (B_1, B_2) квадратных матриц порядка n над полем K *эквивалентны*, если над K существуют такие обратимые квадратные матрицы P и Q порядка n, что $A_1 = PB_1Q$ и $A_2 = PB_2Q$. Показать, что если матрицы A_1 и B_1 обратимы, то для эквивалентности этих пар необходимо и достаточно, чтобы матрицы $XA_1 + A_2$ и $XB_1 + B_2$ были эквивалентны над кольцом $K[X]$.

*4) а) Пусть A и B — квадратные матрицы порядка n над полем K, f_i и g_i $(1 \leqslant i \leqslant n)$ — их инварианты подобия. Показать, что векторное пространство (над полем K) квадратных матриц U порядка n, таких, что $UA = BU$, изоморфно пространству $M_0 = M/N$, определенному следующим образом: M — пространство квадратных матриц $(u_{ij}(X))$ порядка n над $K[X]$, таких, что $u_{ij}(X)\, f_j(X)$ кратно $g_{ij}(X)$ для любых i и j; N — подпространство в M, состоящее из таких матриц $(u_{ij}(X))$, что $u_{ij}(X)$ кратно $g_i(X)$ для любых i и j. (Рассмотреть U, A и B как матрицы эндоморфизмов u, v и w пространства $E = K^n$ и заметить, что u — $K[X]$-линейное отображение модуля E_v в E_w: представить E_v и E_w как фактормодули и воспользоваться упражнением 2 § 2 гл. II).

б) В случае, когда $B = A$, матрицы U, такие, что $UA = AU$, образуют кольцо P; тогда M — некоторое кольцо квадратных матриц, N — его двусторонний идеал и P изоморфно факторкольцу M/N.

Показать, что P совпадает с кольцом $K[A]$, порожденным матрицами I_n и A, тогда и только тогда, когда минимальный многочлен матрицы A равен ее характеристическому многочлену.

в) Показать, что для произвольных матриц A и B размерность пространства M_0 равна $\sum_{i,j} m_{ij}$, где m_{ij} — степень н. о. д. многочленов f_i и q_j (использовать упражнение 8 § 5) (метод упражнения а)).

г) Показать, что наибольший из рангов матриц $U \in M_0$ равен $\sum_k d_k$, где d_k — степень н. о. д. многочленов f_k и g_k (использовать упражнение 8 § 5).

д) Обобщить результаты упражнений а), в) и г) на случай, когда A — квадратная матрица порядка n, B — квадратная матрица порядка m и U — матрица из m строк и n столбцов.

ИСТОРИЧЕСКИЙ ОЧЕРК

К ГЛАВАМ VI и VII

(Римские цифры в скобках относятся к библиографии в конце настоящего очерка.)

Элементарные арифметические операции и в особенности вычисления с дробями не могли не привести к многочисленным наблюдениям эмпирического характера о делимости целых чисел. Однако ни вавилоняне (столь искушенные в алгебре), ни египтяне (с их акробатическими правилами действий при вычислении дробей) не знали, по-видимому, общих законов делимости, и первое слово здесь принадлежит грекам. Их достижения в арифметике, основное изложение которых находится в VII и IX Книгах Евклида (I), ни в какой степени не уступают их лучшим открытиям в других областях математики. В самом начале VII Книги доказывается существование н. о. д. двух целых чисел — с помощью процесса, известного под названием «алгоритм Евклида» *); это утверждение служит отправной точкой для всего дальнейшего развития теории (свойства простых чисел, существование и вычисление н. о. к. и т. д.), основанного на рассуждениях, которые, в сущности, почти не отличаются от рассуждений, проведенных выше, в гл. VI, § 1. И венцом этого здания являются две замечательные теоремы: доказательство существования бесконечного множества простых чисел (Книга IX, предложение 20) и процесс построения четных совершенных чисел исходя из некоторых простых чисел (см. гл. VII, § 1, упражнение 24; как показал Эйлер, этот процесс дает в действительности все четные совершенные числа). Лишь существование и единственность разложения числа на простые множители не были доказаны в общем виде; тем не менее Евклид явно доказывает, что всякое целое число

*) Если a_1 и a_2 — целые числа и $a_1 \geqslant a_2$, то алгоритм определяет a_n (для $n \geqslant 3$) по индукции как остаток от евклидова деления a_{n-2} на a_{n-1}; если m — наименьший индекс, для которого $a_m = 0$, то a_{m-1} является н. о. д. чисел a_1 и a_2. Этот прием является перенесением в область целых чисел метода попеременного вычитания (иногда называемого также ἀνθυφαίρεσις) для нахождения общей меры двух величин. Этот метод восходит, без сомнения, к пифагорейцам и является, по-видимому, основой доевдоксовой теории иррациональных чисел.

делится на простое число (Книга VII, предложение 31), а также следующие два предложения (Книга IX, предложения 13 и 14) *):

«*Если сколько угодно чисел, начиная с единицы, составляют прогрессию с произвольным постоянным отношением* (то есть геометрическую прогрессию) *и следующее за единицей число простое, то наибольшее число не делится ни на какие числа, кроме тех, которые имеются в прогрессии*» (степень простого числа p^n может делиться только на степени p с показателем $\leqslant n$).

«*Если некоторое число является наименьшим, делящимся на* (данные) *простые числа, то оно не делится ни на какое простое число, кроме тех, которые первоначально* (заданы как) *делители*» (другими словами, произведение различных простых чисел $p_1, \ldots, p_k$ не имеет простых множителей, отличных от $p_1, \ldots, p_k$).

Таким образом, складывается представление, что Евклид не формулирует общей теоремы лишь из-за отсутствия подходящей терминологии и обозначений для произвольных степеней целых чисел **).

Хотя внимательное изучение довольно определенно показывает наличие в тексте Евклида нескольких последовательных слоев, каждый из которых соответствует некоторому этапу развития арифметики***), вся эта эволюция происходила с начала V и до середины IV в., и можно лишь восхищаться изяществом и логической надежностью построенных при этом теорий: нужно будет ждать еще два тысячелетия, чтобы присутствовать при сравнимом прогрессе арифметики.

Источником дальнейшего развития теории чисел были проблемы, называемые «неопределенными» или «диофантовыми». Термин «диофантовы уравнения», употребляющийся в настоящее время, исторически не совсем оправдан; под этими уравнениями обычно понимают алгебраические уравнения (или системы уравнений) с целыми коэффициентами, для которых ищутся только целые решения. Эта задача обычно неразрешима, если уравнения «определены», то есть имеют лишь конечное число решений (действительных

---

*) Перевод сделан с французского текста данной книги. (*Прим. перев.*)

**) Для подтверждения этой гипотезы можно также заметить, что доказательство теоремы о совершенных числах является, в сущности, частным случаем теоремы об однозначности разложения на простые множители. Впрочем, все свидетельства сходятся в том, что уже в эту эпоху явное разложение числа на простые множители было известно и свободно использовалось; однако полного доказательства этой теоремы разложения не было вплоть до доказательства Гаусса в начале «Disquisitiones» ((VIII), т. I, стр. 15).

***) См. B. L. van der Waerden, Die Arithmetik der Pythagoreer, Math. Ann., CXX (1947—1949), стр. 127. Примером остатка старых теорий могут служить предложения с 21 по 31 Книги IX, в которых исследуются самые элементарные свойства делимости на 2 и которые, несомненно, относятся к эпохе, когда общая теория простых чисел еще не была развита. Известно, впрочем, что категории четного и нечетного играли большую роль в мистических философских теориях первых пифагорейцев. Естественно поэтому и связать с ними указанный отрывок.

или комплексных), но, напротив, часто допускает решения, если число неизвестных больше числа уравнений. Однако если Диофант и был первым, кто рассматривал «неопределенные» проблемы, то целые решения он разыскивал только в исключительных случаях и чаще всего удовлетворялся нахождением лишь *одного рационального решения* (II). Проблемы этого типа Диофант чаще всего мог решить алгебраическими вычислениями, в которых арифметическая природа неизвестных не играет роли *); теория делимости также играет у него незначительную роль (слова «простое число» встречаются лишь один раз ((II), Книга V, задача 9, т. I, стр. 334, 335), а понятие взаимно простых чисел привлекается лишь для доказательства теоремы о том, что частное двух взаимно простых чисел может быть квадратом лишь в случае, когда каждое из них является квадратом) **).

По-настоящему изучать целые решения неопределенных уравнений начали только в раннем средневековье китайские и индийские математики. Первые пришли к размышлениям этого рода, видимо, при создании календарей (в которых определение общих периодов нескольких циклов астрономических явлений составляет именно «диофантову» проблему первой степени); во всяком случае, им мы обязаны открытием (которое было сделано, без сомнения, между IV и VII вв. н. э.) правила нахождения общих решений линейных сравнений (см. гл. VI, § 1, упражнение 25). Что же касается индийской математики, находившейся с V по XIII вв. в подлинном расцвете, то индийцы умели не только методично (с помощью алгоритма Евклида) изучать системы линейных диофантовых уравнений с произвольным числом неизвестных ***), но и первыми рассмотрели и решили уравнения второй степени и среди них некоторые частные случаи «уравнения Ферма» $Nx^2 + 1 = y^2$ ((III), т. II, стр. 87—307).

---

*) Решая неопределенные задачи, Диофант всегда сводит их к задаче с одним неизвестным с помощью численного выбора остальных неизвестных, делающего возможным решение получаемой задачи. Представляется все же, что этот метод объясняется его обозначениями, которые не позволяли ему оперировать одновременно с несколькими неизвестными; во всяком случае, в процессе вычислений он не упускает из виду сделанные численные подстановки и в случае, когда они не подходят, выписывает условие пригодности подставляемых переменных и решает эту вспомогательную задачу. Другими словами, он пользуется этими подставляемыми численными значениями так, как мы делаем это с параметрами, и в конечном счете все это сводится к разысканию рационального параметрического представления заданного алгебраического многообразия или его подмногообразия (см. (IIbis)).

**) Многие данные свидетельствуют в то же время о более обширных знаниях Диофанта: он знал, например, что уравнение $x^2 + y^2 = n$ не имеет рациональных решений, если n — целое число вида $4k + 3$ (Книга V, задача 9 и Книга VI, задача 14 ((II), т. I, стр. 332—335 и стр. 425; см. также (IIbis), стр. 105—110)).

***) Астрономические задачи также приводили индийцев к изучению такого рода уравнений (см. (III), т. II, стр. 100, 117 и 135).

Мы не прослеживаем здесь всю историю диофантовых уравнений степени >1, которая после работ Ферма, Эйлера, Лагранжа и Гаусса привела к созданию в XIX в. теории целых алгебраических чисел. Как мы уже отмечали (см. Исторический очерк к гл. II и III), изучение систем линейных уравнений, которое, как казалось, не ставит больше интересных проблем, в этот период оставалось в тени: в частности, никто не пытался ни сформулировать общие условия разрешимости произвольной системы уравнений, ни описать множество решений. Однако в середине XIX в. Эрмиту в его исследованиях по теории чисел пришлось использовать некоторые леммы о линейных диофантовых уравнениях, и в особенности «приведенную форму» линейной подстановки с целыми коэффициентами ((XIII), стр. 164 и 265); наконец, после того как в 1858 г. Хегер дал условие разрешимости системы, ранг которой равен числу уравнений, Г. Дж. Смит в 1861 г. определил инвариантные факторы матрицы с целыми элементами и получил общую теорему о приведении такой матрицы к «каноническому виду», рассмотренному нами в гл. VII, § 4, следствие 1 предложения 4 (XVII).

В этот период постепенно уточнялось понятие абелевой группы — после введения его Гауссом (см. Исторический очерк к гл. I, II и III) — благодаря важности этого понятия для дальнейшего развития теории чисел. При особенно углубленном исследовании конечной абелевой группы классов квадратичных форм с данным дискриминантом, изложенном в «Disquisitiones», Гаусс быстро обнаружил, что некоторые из этих групп не являются циклическими: «*В этом случае*,— пишет он,— *единого базиса* (то есть образующего) *может быть недостаточно, и их надо взять два или больше, чтобы с помощью умножения и композиции* *) *они могли бы произвести все остальные классы*» ((VIII), т. I, стр. 374, 375). Нельзя определенно утверждать, что этими словами Гаусс хотел выразить возможность разложения группы в прямое произведение циклических групп; во всяком случае, в той же статье в «Disquisitiones» он доказывает существование в группе элемента, порядок которого равен н. о. к. порядков всех остальных элементов, другими словами, существование наибольшего инвариантного фактора группы ((VIII), т. II, стр. 373); с другой стороны, понятие прямого произведения ему известно, так как в рукописи, датированной в 1801 г., но не опубликованной при его жизни, он намечает общее доказательство разложения конечной абелевой группы в прямое произведение p-групп **) ((VIII), т. II, стр. 266). Во всяком случае, Шеринг, издатель его сочинений, вдохновленный этими результатами (и особенно рукописью, только что им обнаруженной), в 1868 г. доказывает (все для той же группы классов квадратичных форм) общую теорему разложения (XVIII). Его метод, переформулированный в абстрактных терминах Кронекером (XX) двумя годами спустя, совпадает, по существу, с методом, использованным нами выше (гл. VII, § 4, теорема 1). Что касается абелевых

*) Гаусс обозначал закон композиции классов аддитивно, а под «умножением» понимал, следовательно, произведение класса на целое число.

**) Это утверждение мимоходом доказано также Абелем в его мемуаре об абелевых уравнениях ((IX), т. I, стр. 494—497).

групп без кручения, то мы видели уже (см. Исторический очерк к гл. II, III), как теория эллиптических функций и абелевых интегралов, развитая Гауссом, Абелем и Якоби, постепенно приводила к уяснению их структуры: первый и наиболее замечательный пример разложения бесконечной группы в прямую сумму моногенных групп был дан в 1846 г. в мемуаре Дирихле о единицах поля алгебраических чисел (XI). Однако лишь в 1879 г. Фробениус и Штикельбергер обнаружили и явным образом использовали связь между теорией абелевых групп конечного типа и теоремой Смита ((XXIII), § 10).

К этому времени завершилась также теория подобия матриц (с действительными или комплексными коэффициентами). Понятие собственного значения линейной подстановки явно появляется в теории систем линейных дифференциальных уравнений с постоянными коэффициентами, которую Лагранж применял в теории малых движений (VIa) и Лагранж (VIb) и Лаплас (VIIa) — к «вековым» возмущениям планет. Неявно это понятие присутствует и во многих других проблемах, рассматривавшихся еще в середине XVIII в., например при отыскании осей коники или квадрики (осуществленном впервые Эйлером (Va)) или при изучении (также развитом Эйлером (Vb)) главных осей инерции твердого тела (открытых в 1755 г. де Сенье); мы знаем теперь, что это понятие (в гораздо более скрытом виде) встречается в самом начале теории уравнений с частными производными и, в частности, в теории колебаний струны. Однако (если не говорить об этом последнем примере) родство этих различных проблем едва ли было известно до Коши (X). Кроме того, в большей части этих задач используются симметрические матрицы, и поэтому прежде всего в них исследуются именно их собственные значения; за дальнейшими подробностями мы отсылаем к Историческим очеркам к главам этого трактата, посвященным эрмитовым операторам; заметим только, что в 1826 г. Коши доказывает, что собственные значения этих матриц инвариантны относительно подобия и что у симметрических матриц третьего порядка собственные значения действительны (Xa) — этот результат через три года был доказан им для произвольных симметрических действительных матриц (Xb) *). Общее понятие проективности, введенное Мебиусом в 1827 г., быстро привело к проблеме классификации проективных преобразований (прежде всего для размерности 2 и 3) или, что то же самое, к проблеме подобия соответствующих матриц; однако в течение долгого времени этот вопрос исследовался лишь «синтетическими» методами, широко распространенными в середине XIX в., и прогресс в этом направлении, по-видимому, не оказывал

*) Попытка доказательства этого результата для частного случая «вековых» возмущений планет была уже сделана Лапласом в 1784 г. (VIIb). Что касается уравнения третьей степени, задающего оси действительной квадрики, то Эйлер допускает без доказательства, что его корни действительны; попытка Лагранжа провести в 1773 г. (VIe) это доказательство оказалось безуспешной. Впервые это было доказано строго Ашеттом и Пуассоном в 1801 г. (Journal de l'Ecole Polytechnique, тетрадь 11 (an X), стр. 170—172).

влияния на теорию собственных значений. По-иному обстояло дело с другой геометрической задачей — классификацией пучков коник или квадрик, состоящей с современной точки зрения в изучении элементарных делителей матрицы $U + \lambda V$, где U и V — симметрические матрицы. Именно в этом духе подошел к этой проблеме Сильвестр, тщательно исследовавший (для нахождения «канонического вида» рассматриваемого пучка), что происходит с минорами матрицы $U + \lambda V$ при подстановке вместо λ некоторого значения, аннулирующего ее определитель (XIV). В то же время развивался чисто алгебраический аспект теории собственных значений; именно алгебраическими методами многие авторы (и в том числе сам Сильвестр) в 1850 г. доказали, что собственные значения матрицы U^n являются n-ми степенями собственных значений матрицы U, а в 1858 г. Кэли в своем мемуаре, заложившем основы матричного исчисления (XVI), сформулировал «теорему Гамильтона — Кэли» для квадратных матриц произвольного порядка *), удовлетворившись прямым ее доказательством для матриц порядка 2 и 3. Наконец, в 1868 г. Вейерштрасс, пользуясь методом Сильвестра, получает «канонический вид» для «пучка» $U + \lambda V$, где на этот раз матрицы U и V не обязательно симметрические и удовлетворяют единственному условию, чтобы определитель матрицы $U + \lambda V$ не был тождественным нулем; из этого он выводит определение элементарных делителей произвольной квадратной матрицы (с комплексными элементами) и доказывает, что они характеризуют матрицу с точностью до подобия (XIX); кроме того, эти результаты частично были вновь открыты Жорданом (по-видимому, независимо) два года спустя **) (XXI).

И здесь снова Фробениус в 1879 г. показал, что теорему Вейерштрасса можно просто вывести из теории Смита, распространенной на многочлены ((XXII), § 13); его рассуждения основываются на доказательстве этой теоремы, которое мы дали выше (гл. VII, § 5, предложение 5).

Мы только что коснулись теории делимости многочленов от одного переменного. Вопрос о делении многочленов как об операции, обратной умножению (эта операция была известна уже Диофанту), естественно, должен был быть поставлен в самом начале развития алгебры. Ясно, однако, что едва ли возможно решать эту проблему в общем виде до тех пор, пока не создана последовательная система обозначений для различных степеней переменного. Действительно, до середины XVI в. не появляется ни одного

*) Гамильтон по ходу дела доказал эту теорему для матриц порядка 3 несколькими годами раньше ((XV), стр. 566, 567).

**) Жордан не отмечает инвариантности полученного им канонического вида. Интересно, что к тому же он исследует вопрос не для матриц с комплексными элементами, а для матриц над конечным полем. Подчеркнем, с другой стороны, что уже в 1862 г. Грассман дал метод приведения матрицы (с комплексными элементами) к треугольному виду и явно указал на связь между этим приведением и проективными преобразованиями (Ges. Math. Werke, т. I_2, Leipzig (Teubner), 1896, стр. 249—254).

примера «евклидова» деления многочленов *), и, видимо, Стевин (который, в сущности, использовал обозначение показателя) был первым, кто пришел к мысли применить «алгоритм Евклида» для отыскания н. о. д. двух многочленов ((IV), т. I, стр. 54—56). Не считая этого примера, понятие делимости вплоть до середины XVIII в. оставалось принадлежностью теории целых рациональных чисел. Новую главу арифметики открыл Эйлер, отважно распространив в 1770 г. понятие делимости на целые элементы квадратичного расширения: пытаясь найти делители некоторого числа вида $x^2 + cy^2$ (x, y, c — целые рациональные числа), он полагает $x + y\sqrt{-c} = (p + q\sqrt{-c}) \times (r + s\sqrt{-c})$ (p, q, r, s — целые рациональные числа) и, взяв нормы этих чисел, не колеблясь, утверждает, что тем самым он получил все делители числа $x^2 + cy^2$, имеющие вид $p^2 + cq^2$ (Vc). Другими словами, Эйлер рассуждает таким образом, будто $Z[\sqrt{-c}]$ есть кольцо главных идеалов; несколько позже он использует аналогичное рассуждение для применения метода «бесконечного спуска» к уравнению $x^3 + y^3 = z^3$ (дело сводится к записи того, что $p^2 + 3q^2$ является кубом, что Эйлер и делает, полагая $p + q\sqrt{-3} = (r + s\sqrt{-3})^3$). Но уже в 1773 г. Лагранж доказывает (VIc), что делители числа вида $x^2 + cy^2$ не всегда сами имеют такой вид, и это был первый пример принципиальных трудностей, которые гораздо более четко выявились в работах Гаусса и его последователей, относящихся к делимости в полях корней из единицы **); на эти поля, вообще говоря, невозможно непосредственно перенести основные свойства делимости рациональных чисел, существование н. о. д. и единственность разложения на простые множители. Здесь не место описывать, как Куммер при изучении полей корней из единицы (XII) ***), а затем Дедекинд и Кронекер при исследовании произвольных полей алгебраи-

---

*) См., например, H. Bosmans, Sur le «libro del Algebra» de Pedro Nuñez, Bibl. Math. (3), VIII (1907—08), 154—169.

**) Одно время Гаусс, видимо, надеялся, что кольцо целых в поле корней n-й степени из единицы является кольцом главных идеалов; в одной из рукописей, не опубликованных при его жизни ((VIII), т. II, стр. 387—397), он доказывает наличие процесса евклидова деления в поле кубических корней из единицы и дает несколько указаний об аналогичном процессе в поле корней пятой степени; эти результаты он использует для более корректного, чем у Эйлера, доказательства методом «бесконечного спуска» неразрешимости уравнения $x^3 + y^3 = z^3$ в поле кубических корней из единицы, подчеркивает, что этот метод можно применить к уравнению $x^5 + y^5 = z^5$, но останавливается перед уравнением $x^7 + y^7 = z^7$, заметив, что здесь нельзя отбросить a priori случай, когда x, y, z не делятся на 7.

***) Начиная со своей первой работы об «идеальных числах», Куммер явно подчеркивает, что его метод применим не только к полям корней из единицы, но и к квадратичным полям и, таким образом, позволяет заново получить результаты Гаусса о бинарных квадратичных формах ((XII), стр. 324, 325).

ческих чисел сумели преодолеть это грозное препятствие созданием теории идеалов, ставшей решающим достижением современной алгебры. Но Дедекинд, всегда относившийся с большим интересом к обоснованию различных математических теорий, не удовлетворился этим успехом и, анализируя механизм отношений, связанных с делимостью, заложил основы теории решеточно упорядоченных групп в мемуаре (который не нашел отклика у современников и в течение 30 лет оставался забытым), ставшем, без сомнения, одной из первых по времени работ по аксиоматической алгебре (XXIV); если не считать обозначений, то его работа уже очень близка к современному виду этой теории, изложенной нами в гл. VI, § 1.

*

* *

С середины XVIII в. одной из первоочередных задач было доказательство «основной теоремы алгебры» (см. Исторический очерк к гл. IV и V). Мы не будем здесь напоминать о попытке Даламбера, которая привела к целой серии доказательств, использующих исчисление бесконечно малых (см. Общ. топол., Исторический очерк к гл. VIII). Но в 1749 г. Эйлер подошел к этой проблеме совершенно по-иному (Vd): для любого многочлена f с действительными коэффициентами он пытается доказать существование разложения $f = f_1 f_2$ на два многочлена (отличных от постоянной) с действительными коэффициентами, откуда он смог бы получить доказательство «основной теоремы» индукцией по степени многочлена f. При этом даже достаточно, отмечает он, остановиться на первом множителе нечетной степени, и поэтому вся трудность состоит в рассмотрении случая, когда многочлен f имеет четную степень n. В этом случае Эйлер ограничивается нахождением множителей, каждый из которых имеет степень $n/2$, и указывает, что с помощью подходящего исключения неизвестные коэффициенты многочленов f_1, f_2 можно рациональным образом выразить как функции от корня некоторого уравнения с действительными коэффициентами, первый и последний член которого имеют *противоположные знаки* и которое имеет, следовательно, по крайней мере один действительный корень. Однако доказательство Эйлера является лишь наброском, и многие существенные моменты обходятся в нем молчанием; лишь в 1772 г. Лагранжу удалось преодолеть трудности, возникшие при этом в доказательстве (VId), и сделал он это чрезвычайно длинным и кропотливым путем, виртуозно используя созданные им методы «теории Галуа» (см. Исторический очерк к гл. IV и V).

Тем не менее Лагранж, подобно Эйлеру и его современникам, без всяких колебаний проводил формальные рассуждения в «поле корней» многочлена (то есть на его языке, он рассматривал «мнимые корни» этого многочлена). Никакого обоснования подобных методов рассуждений математика времени Лагранжа еще не давала. Гаусс, с самого начала бывший решительным противником безудержного формализма XVIII в., в своей диссертации со всей силой обрушился на эти вольности ((VIII), т. III, стр. 3). Но Гаусс не был

бы самим собой, если бы не почувствовал, что речь идет здесь лишь о внешне неполном изложении правильных в своей основе рассуждений. И мы видим, как несколько лет спустя ((VIII), т. III, стр. 33; см. также (VIII bis)) Гаусс проводит более простой вариант доказательства Эйлера, намеченный еще в 1759 г. Фонсене (который, однако, не смог хорошо его провести), и выводит из него новое доказательство «основной теоремы», в котором заботливо избегает какого бы то ни было использования «мнимых» корней: вместо этого он умело пользуется присоединением и специализацией переменных. По существу, именно это доказательство Гаусса и дано нами в тексте (гл. VI, § 2, теорема 3), лишь с упрощениями благодаря использованию алгебраических расширений.

Таким образом, роль топологии в доказательстве «основной теоремы» оказывается сведенной к единственной теореме, согласно которой многочлен с действительными коэффициентами не может изменить знак на интервале, не обратившись в нуль (теорема Больцано для многочленов). На этой теореме основываются также все критерии отделения корней действительных многочленов (с действительными коэффициентами), составляющие излюбленную тему алгебры XIX в. *). В ходе этих исследований нельзя было не заметить, что существенную роль в этом играет не столько топология поля $\boldsymbol{R}$, сколько его структура порядка **); например, теорема Больцано для многочленов остается верной для поля всех действительных алгебраических чисел. Это развитие идей нашло свое завершение в абстрактной теории упорядоченных полей, созданной Э. Артином и О. Шрейером (XXV); самым замечательным результатом этой теории является, без сомнения, открытие существования в поле отношения порядка, связанного с чисто алгебраическими свойствами этого поля. Именно эта теория и изложена в § 2 гл. VI.

---

*) По вопросам, не затронутым нами в этом очерке, отсылаем читателя, например, к книгам J.-A. Serret, Cours d'Algèbre supériere, 3e éd., Paris (Gauthier-Villars), 1866, B. L. van der Waerden, Moderne Algebra, т. I, (1re éd.), Berlin (Springer), 1930, стр. 223—235.

**) Тенденция придавать структуре порядка действительных чисел преобладающее значение сказывается также в определении действительных чисел с помощью дедекиндовых «сечений», в основе которого лежит процесс, применимый ко всем упорядоченным множествам (см. Книга I, гл. III и Книга II, гл. VI, § 1, упражнение 30 и далее).

БИБЛИОГРАФИЯ

(I) Euclidis Elementa, 5 тт., éd. J. L. Heiberg, Lipsiae (Teubner)

(I bis) T. L. Heath, The thirteen books of Euclid's Elements..., 3 тт. Cambridge, 1908.

(II) Diophanti Alexandrini Opera Amnia..., 2 тт., éd. P. Tannery, Lipsiae (Teubner), 1893—1895.

(II bis) T. L. Heath, Diophantus of Alexandria, 2e éd., Cambridge, 1910.

(III) B. Datta and A. N. Singh, History of Hindu mathematics, 2 тт., Lahore (Motilal Banarsi Das), 1935—1938.

(IV) S. Stevin, Les œuvres mathématiques..., éd. A. Girard, Leyde (Elsevier), 1634, т. I.

(V) L. Euler: a) Introductio in Analysin Infinitorum (Opera Omnia (1), т. IX, Zürich—Leipzig—Berlin (O. Füssli et B. G. Teubner), 1945, стр. 384); b) Theoria motus corporum solidorum seu rigidorum (Opera Omnia (2), т. III, Zürich—Leipzig—Berlin (O. Füssli et B. G. Teubner), 1948, стр. 200, 201); c) Vollständige Anleitung zur Algebra (Opera Omnia (1), т. I, Leipzig—Berlin (Teubner), 1911, стр. 422); d) Recherches sur les racines imaginaires des équations (Opera Omnia (1), т. VI, Leipzig — Berlin (Teubner), 1921, стр. 78).

(VI) J.-L. Lagrange, Œuvres, Paris (Gauthier-Villars), 1867—1892: a) Solutions de divers problèmes de Calcul intégral, т. I, стр. 520; b) Recherches sur les équations séculaires du mouvement des nœuds, т. VI, стр. 655—666; c) Recherches d'arithmétique, т. III, стр. 695—795; d) Sur la forme des racines imaginaires des équations, т. III, стр. 479; e) Nouvelle solution du problème de rotation d'un corps quelconque qui n'est animé par aucune force accélératrice, т. III, стр. 579—616.

(VII) P. S. Laplace: a) Mémoire sur les solutions particulières des équations différentielles et sur les inégalités séculaires des planètes (Œuvres, т. VIII, Paris (Gauthier-Villars), стр. 325—366); b) Mémoire sur les inégalités séculaires des planètes et des satellites (Œuvres, т. XI, Paris (Gauthier-Villars), 1895, стр. 49—92).

(VIII) C. F. Gauss, Werke, т. I (Göttingen, 1870), т. II (ibid., 1876) et т. III (ibid., 1876).

(VIII bis) Die vier Gauss'schen Beweise für die Zerlegung ganzer algebraischer Functionen in reelle Factoren ersten oder zweiten Grades (Ostwald's Klassiker, n° 14, Leipzig (Teubner), 1904).

(IX) N. H. Abel, Œuvres, т. I, éd. Sylow et Lie, Christiania, 1881.

(X) A. L. Cauchy: a) Leçons sur les applications du Calcul infinitésimal à la Géométrie (Œuvres complètes (2), т. V, Paris (Gauthier-Villars), 1903, стр. 248); b) Sur l'équation à l'aide de laquelle on détermine les inégalités séculaires des planètes (Œuvres complètes (2), т. IX, Paris (Gauthier-Villars), 1891, стр. 174.

(XI) P. G. Lejeune-Dirichlet, Werke, т. I, Berlin (G. Reimer), 1889, стр. 619—644.

(XII) E. Kummer, Zur Theorie der complexen Zahlen, J. de Crelle, XLIII, p. 319 (1847).

(XIII) Ch. Hermite, Œuvres, т. I, Paris (Gauthier-Villars), 1905.

(XIV) J. J. Sylvester, Collected Mathematical Papers, т. I, Cambridge, 1904: An enumeration of the contacts of lines and surfaces of the second order, стр. 219 (= Phil. Mag., 1851).

(XV) W. R. Hamilton, Lectures on Quaternions, Dublin, 1953.

(XVI) A. Cayley, Collected Mathematical Papers, Cambridge, 1889—1898: A memoir on the theory of matrices, т. II, стр. 475—496 (= Phil. Trans., 1858).

(XVII) H. J. Smith, Collected Mathematical Papers, т. I, Oxford, 1894: On systems of linear indeterminate equations and congruences, str. 367. (= Phil. Trans., 1861).

(XVIII) E. Schering, Die fundamental Classen der zusammengesetzbaren arithmetischen Formen, Abh. Ges. Göttingen, XIV, 13 (1868—1869).

(XIX) K. Weierstrass, Mathematische Werke, т. II, Berlin (Mayer und Müller), 1895: Zur Theorie der bilinearen und quadratischen Formen, стр. 19.

(XX) L. Kronecker, Auseinandersetzungen einiger Eigenschaften der Klassenanzahl idealer complexer Zahlen, Monats. Abhandl. Berlin (1870), стр. 881 (= Werke, т. I, Leipzig (Teubner), 1895, стр. 273).

(XXI) C. Jordan, Traité des substitutions et des équations algébriques, Paris (Gauthier-Villars), 1870, стр. 114—125.

(XXII) G. Frobenius, Theorie der linearen Formen mit ganzen Coefficienten, J. de Crelle LXXXVI, 146 (1879).

(XXIII) G. Frobenius und L. Stickelberger, Ueber Gruppen von vertauschbaren Elementen, J. de Crelle LXXXVI, 217 (1879).

(XXIV) R. Dedekind, Gesammelte mathematische Werke, т. II, Braunschweig (Vieweg), 1932: Ueber Zerlegungen von Zahlen durch ihre grössten gemeinsamen Teiler, стр. 103.

(XXV) a) E. Artin und O. Schreier, Algebraische Konstruktion reeller Körper, Abh. Math. Sem. Univ. Hamburg V, 83 (1927); b) E. Artin, Ueber die Zerlegung definiter Funktionen in Quadrate (ibid., стр. 100); c) E. Artin und O. Schreier, Eine Kennzeichnung der reell abgeschlosenen Körper (ibid., стр. 225).

ГЛАВА VIII

ПОЛУПРОСТЫЕ МОДУЛИ И КОЛЬЦА

Все кольца, рассматриваемые в этой главе (исключая приложение), предполагаются кольцами с единицей (обозначаемой обычно 1), *а все модули — унитарными; все рассматриваемые модули, если не оговорено противное, предполагаются левыми. Для всякой алгебры A над полем K, если не оговорено противное, поле K отождествляется с подалгеброй $K \cdot 1$ центра алгебры A* (гл. II, § 7, n° 4); *таким образом, всякий A-модуль при сужении кольца скаляров до K наделяется структурой векторного пространства над полем K.*

§ 1. Коммутирование

1. *Проектирования*

Определение 1. *Пусть A — кольцо M — A-модуль и $L = \mathscr{L}_A(M)$ — кольцо эндоморфизмов модуля M. Элемент $e \in L$ называется проектированием (в M), если $e^2 = e$* (иными словами, *e — идемпотент* кольца L (гл. I, § 1, n° 4)).

В дальнейшем будет удобно для всякого гомоморфизма u A-модуля M в A-модуль N подмодуль $u(M)$ модуля N называть, допуская вольность речи, образом гомоморфизма u.

Предложение 1. *Пусть A — некоторое кольцо, M — A-модуль, $L = \mathscr{L}_A(M)$, e — проектирование в M. Пусть $N = e(M)$ — образ эндоморфизма e и $P = e^{-1}(0)$ — его ядро.*

а) *Модуль M есть прямая сумма N и P.*

б) *Для всякого элемента $x \in M$, имеющего вид $x_1 + x_2$, где $x_1 \in N$, $x_2 \in P$, выполняется равенство $e(x) = x_1$.*

в) *Элемент* 1 — e *является проектированием, его образ есть P, а ядро — N.*

г) *Правый идеал eL есть множество элементов $u \in L$, образ которых содержится в N; левый идеал Le есть множество элементов $u \in L$, ядро которых содержит P.*

Из равенства $(1-e)^2 = 1 - 2e + e^2 = 1 - e$ следует, что $1 - e$ — проектирование. Пусть $x \in M$. Элемент x принадлежит N тогда и только тогда, когда $x = e(x)$; достаточность этого условия очевидна, а необходимость следует из того, что если $x = e(x')$, то $e(x) = e^2(x') = e(x') = x$. Это показывает, что N является ядром проектирования $1 - e$. Меняя ролями e и $1 - e$, можно убедиться в справедливости утверждения в). Формула

$$y = e(y) + (1-e)(y), \tag{1}$$

справедливая для всех $y \in M$, показывает, что $M = N + P$. Если $z \in N \cap P$, то $z = e(z)$ и $e(z) = 0$, так что $N \cap P = \{0\}$. Это доказывает утверждение а); утверждение б) следует тогда из формулы (1). Наконец, пусть $c \in L$; включение $C(M) \subset N$ справедливо тогда и только тогда, когда $(1 - e)c = 0$, то есть $c \in eL$; $c^{-1}(0) \supset P$ тогда и только тогда, когда $c(1 - e) = 0$, то есть $c \in Le$. Это заканчивает доказательство.

Обратно, пусть M — A-модуль, N и P — дополнительные подмодули в M. Для любого $x = x_1 + x_2$, $x_1 \in N$, $x_2 \in P$, положим $e(x) = x_1$ (*компонента* x в N (гл. II, § 1, п° 7)). Ясно, что e — единственное проектирование в M, имеющее ядро P и образ N. Проектирование e называется *проектированием модуля M на N.*

Определение 2. *Пусть некоторое A — кольцо, M — A-модуль, N — его подмодуль. Подмодуль N называется прямым слагаемым в модуле M, если N имеет в M дополнение.*

В соответствии с предыдущим для этого необходимо и достаточно, чтобы в модуле M существовало проектирование, у которого образ или ядро совпадает с N.

Если N — прямое слагаемое в модуле M, то всякий гомоморфизм u подмодуля N в A-модуль P продолжается до гомоморфизма модуля M в P, например до гомоморфизма $u \circ e$ (e — проектирование M на N). Обратно, если тождественное отображение подмодуля N продолжается до гомоморфизма f модуля M в N, то $f \circ f = f$, так что f — проектирование модуля M на N, и N — прямое слагаемое в M.

Пусть M и M' — A-модули, u — гомоморфизм модуля M в M', v — гомоморфизм модуля M' в M. Если $v \circ u$ — тождественное отображение модуля M, то $u \circ v$ — проектирование в M', u — изоморфизм модуля M на $u(M)$, v отображает M' на M, и модуль M' есть прямая сумма подмодулей $u(M)$ и $v^{-1}(0)$, являющихся, таким образом, прямыми слагаемыми в M'.

Определение 3. *Семейство $(e_\iota)_{\iota \in I}$ идемпотентов некоторого кольца называется ортогональным семейством, если при $\iota \neq \varkappa$ выполняется равенство $e_\iota e_\varkappa = 0$.*

Пусть M — A-модуль, являющийся прямой суммой семейства $(M_\iota)_{\iota \in I}$ своих подмодулей, и $e_\iota(x)$, $x \in M$,— компонента элемента x в M_ι; тогда e_ι — проектирование, его образ есть M_ι, а ядро $\sum_{\iota \in I} M_\iota$. Семейство $(e_\iota)_{\iota \in I}$ ортогонально, так как при $\iota \neq \varkappa$, $x \in M$ имеем $e_\varkappa(x) \in M_\varkappa$, и следовательно, $e_\iota e_\varkappa(x) = 0$. $(e_\iota)_{\iota \in I}$ называется *семейством проектирований, ассоциированным с разложением модуля M в прямую сумму* $\sum_{\iota \in I} M_\iota$.

Обратно:

Предложение 2. *Пусть M — A-модуль, $(e_\iota)_{\iota \in I}$ — ортогональное семейство проектирований модуля M, обладающее следующим свойством: $e_\iota(x) = 0$ для любого $x \in M$ и для всех индексов $\iota \in I$, кроме конечного числа, и $x = \sum_{\iota \in I} e_\iota(x)$. Тогда M является прямой суммой подмодулей $M_\iota = e_\iota(M)$ и $(e_\iota)_{\iota \in I}$ — семейство проектирований, ассоциированное с разложением модуля M в прямую сумму* $\sum_{\iota \in I} M_\iota$.

В самом деле, равенство $M = \sum_{\iota \in I} M_\iota$ очевидно. Пусть элементы $y_\iota \in M_\iota$ все, кроме конечного числа, равны нулю и $\sum_{\iota \in I} y_\iota = 0$; тогда $\sum_{\iota \in I} e_\iota(y_\iota) = 0$, откуда для любого индекса $\varkappa$ следует равенство

$$0 = e_\varkappa\left(\sum_{\iota \in I} e_\iota(y_\iota)\right) = e_\varkappa(e_\varkappa(y_\varkappa)) = e_\varkappa(y_\varkappa) = y_\varkappa.$$

Это показывает, что сумма $\sum_{\iota \in I} M_\iota$ прямая. Последнее утверждение предложения очевидно.

2. Коммутант и бикоммутант

Определение 4. *Пусть X — кольцо и A — подмножество в X. Коммутантом (или централизатором) множества A в X называется подкольцо A' кольца X, состоящее из всех элементов, перестановочных со всеми элементами множества A. Коммутант A'' множества A в X называется бикоммутантом множества A в X.*

Имеет место включение $A \subset A''$. Следовательно, A' содержится в своем бикоммутанте, который есть не что иное, как коммутант B множества A'; но из включения $A \subset A''$ следует, что $A' \supset B$, то есть множество A' совпадает со своим бикоммутантом.

Если множество A является подкольцом в X, то его центр равен $A \cap A'$. Если, кроме того, кольцо A коммутативно, то $A \subset A'$ и, следовательно, $A' \supset A''$; таким образом, в этом случае центр кольца A' равен A''.

Если X — алгебра над полем K (которое можно отождествить с некоторым подполем центра алгебры X), то коммутант любого ее подмножества является в X подалгеброй.

Предложение 3. *Пусть A* (соответственно B) *— алгебра над полем K, C* (соответственно D) *— подалгебра в A* (соответственно *в B*), *C'* (соответственно *D'*) *— коммутант подалгебры C* (соответственно D) *в A* (соответственно *в B*). *Тогда коммутант подалгебры $C \otimes_K D$ в $A \otimes_K B$ равен $C' \otimes_K D'$.*

Необходимо доказать, что всякий элемент $z = \Sigma_i a_i \otimes b_i$ коммутанта $C \otimes_K D$ входит в $C' \otimes_K D'$; рассматривая подпространства, дополнительные к C' и D', в A и B соответственно, можно убедиться (гл. III, § 1, n° 3, предложение 7), что $C' \otimes_K D'$ является пересечением $C' \otimes_K B$ и $A \otimes_K D'$. Элементы b_i можно предполагать независимыми; для любого $x \in C$ должно быть справедливо равенство $(x \otimes 1)\, z = z\, (x \otimes 1)$, то есть $\Sigma_i (xa_i - a_i x) \otimes b_i = 0$; отсюда $xa_i - a_i x = 0$ для любого $x \in C$ (гл. III, § 1, n° 3, следствие 1 предложения 7), то есть $a_i \in C'$ для любого индекса i, и следовательно, $z \in C' \otimes_K B$; аналогично доказывается включение $z \in A \otimes_K D'$.

Следствие. *Пусть Z и Z' — центры соответственно алгебр A и B. Тогда центр алгебры $A \otimes_K B$ равен $Z \otimes_K Z'$.*

Пусть A — кольцо, M — левый A-модуль, Ω — кольцо эндоморфизмов структуры абелевой группы модуля M. Гомотетия $x \to ax$, $a \in A$, является элементом группы Ω и обозначается a_M. Отображение $a \to a_M$ есть гомоморфизм кольца A на некоторое подкольцо в Ω, называемое *кольцом гомотетий* модуля M и обозначаемое A_M. Допуская вольность речи, коммутант (соответственно бикоммутант) подкольца A_M в Ω называют *коммутантом* (соответственно *бикоммутантом*) *модуля* M. Коммутант модуля M совпадает с кольцом $\mathscr{L}_A(M)$ эндоморфизмов этого модуля.

Определение 5. *Пусть M — левый модуль над кольцом A. Контрмодулем модуля M называется левый модуль над коммутантом $\mathscr{L}_A(M)$, абелева группа которого есть M, и для любых $x \in M$ и $c \in \mathscr{L}_A(M)$ $c \cdot x = c(x)$.*

Пусть A — кольцо. *Левым* (соответственно *правым*) *умножением на элемент* $x \in A$ называется эндоморфизм L_x (соответственно R_x) абелевой группы кольца A, определяемый равенством $L_x(y) = xy$ (соответственно $R_x(y) = yx$). Напомним (гл. II, § 1, п° 1, пример 1), что так определяется на A структура левого A-модуля A_s и структура правого A-модуля A_d; модуль A_d можно также рассматривать как левый модуль над кольцом A^0, противоположным кольцу A; множество A, наделенное этой структурой левого A^0-модуля, обозначается A_r.

Предложение 4. *Пусть A — кольцо. Коммутант модуля A_s* (соответственно A_r) *совпадает с кольцом правых* (соответственно *левых*) *умножений кольца A.*

В самом деле, если $c \in \mathscr{L}_A(A_s)$ и $y \in A$, то $c(y) = c(y \cdot 1) = yc(1) = R_{c(1)}(y)$, так что c есть правое умножение на $c(1)$; обратно, для любого $x \in A$ правое умножение R_x, очевидно, принадлежит $\mathscr{L}_A(A_s)$. Аналогично проверяется, что $\mathscr{L}_{A^0}(A_r)$ является кольцом левых умножений кольца A.

Следствие. *Кольцо гомотетий модуля A_s* (соответственно A_r) *совпадает с его бикоммутантом.*

Заметим, что отображение $x \to L_x$ (соответственно $x \to R_x$) представляет собой *изоморфизм* кольца A на кольцо его левых

умножений (соответственно кольца A^0 на кольцо правых умножений кольца A); это следует из того, что равенство $L_x = 0$ (соответственно $R_x = 0$) влечет $L_x(1) = x = 0$ (соответственно $R_x(1) = x = 0$).

3. *Прямые множители и бикоммутанты*

Предложение 5. *Пусть M — A-модуль, B — его бикоммутант, N — прямое слагаемое в M.*

а) *Подмодуль N устойчив относительно B.*

б) *Для любого $b \in B$ сужение b_N эндоморфизма b на N содержится в бикоммутанте A-модуля N.*

в) *Если N' — прямой множитель в M, то всякое A-линейное отображение подмодуля N в N' также и B-линейно.*

Пусть p — проектирование модуля M на N. Если $b \in B$, то b перестановочен с p, и следовательно, $b(N) = b(p(M)) = p(b(M)) \subset p(M) = N$, откуда следует утверждение а). Пусть $\cdot$ — A-линейное отображение модуля N в N'; тогда $c \circ p \in \mathscr{L}_A(M)$, так что, по определению B, композиция $c \circ p$ является B-линейным отображением модуля M в себя; отсюда следует утверждение в). В частности, при $N = N'$ всякий эндоморфизм A-модуля N является также эндоморфизмом B-модуля N, откуда следует, что сужения на N элементов кольца B принадлежат бикоммутанту A-модуля N.

Отображение $b \to b_N$, определенное в предложении 5, является гомоморфизмом кольца B в бикоммутант модуля N и называется *каноническим*. Этот гомоморфизм, вообще говоря, не будет ни инъективным, ни сюръективным (предложение 4).

Лемма 1. *Пусть N и P — A-модули, M — их произведение, B — бикоммутант модуля M. Предположим, что модуль P является суммой подмодулей, изоморфных фактормодулям модуля N. Тогда канонический гомоморфизм кольца B в бикоммутант модуля N* (если N отождествлен с некоторым подмодулем в M) *инъективен. Если, кроме того, бикоммутант модуля N совпадает с кольцом A_N гомотетий модуля N, то B совпадает с кольцом A_M гомотетий модуля M.*

В самом деле, пусть $b \in B$ и $b_N = 0$. Обозначим через L ядро эндоморфизма b. Тогда $N \subset L$ и, по предположению, контр-

модуль модуля M *порождается* модулем N; так как B является кольцом эндоморфизмов этого контрмодуля, то $b = 0$, что доказывает первое утверждение. Если теперь b — произвольный элемент кольца B, и бикоммутант модуля N равен A_N, то существует элемент $\alpha \in A$ такой, что $b_N = \alpha_N$; это равенство можно переписать в виде $(b - \alpha_M)_N = 0$, откуда по предыдущему $b = \alpha_M$.

Предложение 6. *Пусть M — свободный A-модуль. Бикоммутант B модуля M совпадает с кольцом A_M гомотетий модуля M.*

Если $M = \{0\}$, то предложение тривиально. В противном случае модуль M изоморфен некоторому модулю вида $A_s \times P$, где P — сумма модулей, изоморфных A_s. Тогда предложение следует из леммы 1 и следствия предложения 4.

Заметим, что мы заново получаем теорему о строении центра кольца эндоморфизмов свободного модуля (гл. II, § 2, n° 5, следствие 1 предложения 5).

Предложение 7. *Пусть M — модуль конечного типа над кольцом главных идеалов A. Бикоммутант модуля M совпадает с кольцом A_M гомотетий модуля M.*

В самом деле, модуль M изоморфен конечной прямой сумме $\sum_{k=1}^{m} A_s/\mathfrak{a}_k$, где $\mathfrak{a}_k$ — идеалы кольца A и $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \ldots \supset \mathfrak{a}_m$ (гл. VII, § 4, n° 3, теорема 2). При $k \leqslant m-1$ модули $A_s/\mathfrak{a}_k$ изоморфны фактормодулям модуля $A_s/\mathfrak{a}_m$; с другой стороны, модуль $A_s/\mathfrak{a}_m$ имеет то же самое кольцо гомотетий, что и $(A/\mathfrak{a}_m)_s$. Тогда предложение следует из леммы 1 и следствия предложения 4.

Следствие. *Пусть E — конечномерное векторное пространство над полем K, и u — эндоморфизм пространства E. Эндоморфизм v пространства E имеет вид $p(u)$, где p — многочлен из кольца $K[X]$, тогда и только тогда, когда он перестановочен со всеми эндоморфизмами пространства E, перестановочными с u.*

В самом деле, положив $p \cdot x = p(u)\,x$ для любых $p \in K[X]$ и $x \in E$, на пространстве E можно определить структуру модуля конечного типа над кольцом главных идеалов $K[X]$ (гл. VII, § 5, n° 1). Коммутантом этого модуля будет кольцо эндоморфиз-

мов пространства E, перестановочных с u. Поэтому достаточно применить предложение 7.

Определение 6. *Пусть F — модуль над кольцом A. A-модуль M называется изотипным типа F, если M есть прямая сумма семейства подмодулей, изоморфных F.*

Предложение 8. *Пусть A-модуль M является прямой суммой семейства $(F_\iota)_{\iota\in I}$ попарно изоморфных подмодулей, и F — один из этих подмодулей* (отсюда следует, что модуль изотипный типа F). *Пусть B — бикоммутант модуля M. Канонический гомоморфизм кольца B в бикоммутант модуля F биективен. Если рассматривать M и F как B-модули, то модуль M также будет изотипным типа F.*

Модули F_ι являются B-подмодулями модуля M (предложение 5а)) и попарно изоморфны (предложение 5в)); поэтому, если рассматривать M и F как B-модули, то M будет изотипным типа F. По лемме 1 канонический гомоморфизм $b \to b_F$ инъективен. Покажем, что он сюръективен. Пусть f_ι, $\iota \in I$,— изоморфизм модуля F на F_ι (тождественный для $F_\iota = F$), b' — элемент бикоммутанта A-модуля F; очевидно, элемент $b_\iota = f_\iota \circ b'$ принадлежит бикоммутанту модуля F_ι. Существует единственный эндоморфизм b абелевой группы M, сужение которого на каждый модуль F_ι равно b_ι; для завершения доказательства покажем, что $b \in B$. Пусть c — элемент коммутанта модуля M, $x \in F_\varkappa$ и (p_ι) — семейство проектирований, ассоциированное с разложением $M = \sum_\iota F_\iota$. Существует элемент $y \in F$ такой, что $x = f_\varkappa(y)$. Тогда

$$cb(x) = cbf_\varkappa(y) = cb_\varkappa f_\varkappa(y) = cf_\varkappa b'(y)$$

и

$$bc(x) = bcf_\varkappa(y) = \sum_\iota b_\iota p_\iota c f_\varkappa(y) = \sum_\iota (f_\iota b' f_\iota^{-1} p_\iota c f_\varkappa)(y).$$

Однако $f_\iota^{-1} p_\iota c f_\varkappa$ является эндоморфизмом A-модуля F и, следовательно, перестановочен с b'. Поэтому $bc(x) = \sum_\iota p_\iota c f_\varkappa b'(y) = cf_\varkappa b'(y) = cb(x)$. Отсюда по линейности следует равенство $bc = cb$.

Заметим, что предложение 6 является частным случаем предложения 8, соответствующим $F = A_s$.

4. *Предварительные замечания о коммутировании в изотипных модулях*

В этом и следующих пунктах рассматриваются фиксированный A-модуль F и его коммутант C. Мы определим два преобразования, одно из которых переводит правый C-модуль в левый A-модуль, а другой — левый A-модуль в правый C-модуль.

1) *Операция $S(V)$.* Пусть V — *правый C-модуль*; допуская вольность в обозначениях, через $V \otimes_C F$ обозначим тензорное произведение (относительно C) модуля V и контрмодуля модуля F (являющегося левым модулем над C). Напомним (гл. III, приложение II, n° 3), что произведение $V \otimes_C F$ канонически наделяется структурой *левого A-модуля*, для которой

$$a \cdot (v \otimes x) = v \otimes (ax) \tag{2}$$

при любых $a \in A$, $v \in V$, $x \in F$. Множество $V \otimes_C F$, наделенное указанной структурой, обозначается $S(V)$.

Пусть f — C-гомоморфизм модуля V в правый C-модуль V'; легко проверить, что отображение $f \otimes 1$ произведения $V \otimes_C F$ в $V' \otimes_C F$ является A-гомоморфизмом модуля $S(V)$ в $S(V')$. Это отображение обозначается через $S(f)$. Отображение $f \to S(f)$ множества $\mathscr{L}_C(V, V')$ в $\mathscr{L}_A(S(V), S(V'))$ называется каноническим. Справедливы следующие формулы:

$$S(f+f') = S(f) + S(f'), \quad S(f' \circ f) = S(f') \circ S(f), \quad S(1) = 1 \tag{3}$$

(где в первой формуле $f' \in \mathscr{L}_C(V, V')$, во второй $f' \in \mathscr{L}_C(V', V'')$, V'' — правый C-модуль, и в третьей первая 1 есть единичный элемент в $\mathscr{L}_C(V)$, вторая — единичный элемент в $\mathscr{L}_A(S(V))$).

2) *Операция $T(M)$.* Пусть M — *левый A-модуль*. Напомним (гл. III, приложение II, n° 7), что множество $\mathscr{L}_A(F, M)$-гомоморфизмов модуля F в M канонически наделяется структурой *правого C-модуля*, для которой

$$u \cdot c = u \circ c, \tag{4}$$

где $u \in \mathscr{L}_A(F, M)$, $c \in C$. Множество $\mathscr{L}_A(F, M)$, наделенное этой структурой, обозначается $T(M)$.

Пусть g — A-гомоморфизм модуля M в левый A-модуль M'; легко проверить, что отображение $u \to g \circ u$ множества $\mathscr{L}_A(F, M)$ в $L_A(F, M')$ является C-гомоморфизмом модуля $T(M)$ в $T(M')$. Это отображение обозначается $T(g)$. Отображение $g \to T(g)$

множества $\mathscr{L}_A(M, M')$ в $\mathscr{L}_C(T(M), T(M'))$ называется каноническим. Справедливы следующие формулы:

$$T(g+g') = T(g)+T(g'), \quad T(g'\circ g) = T(g')\circ T(g), \quad T(1) = 1 \tag{5}$$

(где в первой формуле $g' \in \mathscr{L}_A(M, M')$, во второй $g' \in \mathscr{L}_A(M', M'')$, M'' — левый A-модуль, и в третьей первая 1 есть единичный элемент в $\mathscr{L}_A(M)$, вторая — единичный элемент в $\mathscr{L}_C(T(M))$).

3) *Соотношения между S и T.* По формуле (2) отображение $x \to v \otimes x$ при любом $v \in V$ является A-гомоморфизмом модуля F в $S(V)$ (обозначения те же, что и выше); обозначим это отображение через $\alpha_V(v)$; при любом $c \in C$ имеем равенство $\alpha_V(vc)(x) = (vc) \otimes x = v \otimes cx = \alpha_V(v)(cx)$. Другими словами, в модуле $T(S(V)) = \mathscr{L}_A(F, S(V))$ выполняется равенство $\alpha_V(vc) = \alpha_V(v)\cdot c$, показывающее, что α_V есть C-гомоморфизм модуля V в $T(S(V))$; этот гомоморфизм называется *каноническим*. Если, кроме того, $f \in \mathscr{L}_C(V, V')$, то

$$\alpha_{V'}\circ f = T(S(f))\circ \alpha_V. \tag{6}$$

В самом деле, $\alpha_{V'}(f(v))$, $v \in V$, является отображением $x \to f(v) \otimes x$ модуля F в $S(V')$, тогда как $T(S(f))(\alpha_V(v))$ есть отображение $S(f)\circ\alpha_V(v)$ модуля F в $S(V')$, то есть отображение $x \to (f \otimes 1)(v \otimes x) = f(v) \otimes x$, что и доказывает равенство (6).

С другой стороны, при $u \in T(M)$, $x \in F$ и $c \in C$ по формуле (4) выполняются равенства

$$(u\cdot c)(x) = u(cx),$$

и следовательно, Z-билинейное отображение $(u, x) \to u(x)$ произведения $T(M) \times F$ в M определяет Z-линейное отображение β_M тензорного произведения $T(M) \otimes_C F$ в M, удовлетворяющее условию $\beta_M(u \otimes x) = u(x)$ (гл. III, приложение II, предложение 1); если $a \in A$, то $\beta_M(a\cdot(u \otimes x)) = \beta_M(u \otimes ax) = u(ax) = au(x) = a\beta_M(u \otimes x)$, так что β_M является A-гомоморфизмом модуля $S(T(M))$ в M; этот гомоморфизм называется *каноническим*. Если, кроме того, $g \in \mathscr{L}_A(M, M')$, то

$$g\circ\beta_M = \beta_{M'}\circ S(T(g)). \tag{7}$$

В самом деле, при $u \in T(M)$ и $x \in F$ имеем равенства

$$(g\circ\beta_M)(u \otimes x) = g(u(x)) = (g\circ u)(x) = \beta_{M'}((g\circ u) \otimes x) =$$
$$= \beta_{M'}((T(g) \otimes 1)(u \otimes x)) = (\beta_{M'}\circ S(T(g)))(u \otimes x).$$

5. Коммутирование в изотипных модулях

В случае, когда A-модуль F *конечного типа*, мы применим операции, введенные в предыдущем пункте для описания изотипного A-модуля M типа F и его коммутанта, рассматривая только структуры A-модулей F и M (но не конкретное разложение модуля M в прямую сумму подмодулей, изоморфных F).

Теорема 1. *Пусть F — левый A-модуль конечного типа и C — его коммутант.*

а) *Пусть V — свободный правый C-модуль, $(v_\iota)_{\iota\in I}$ — его базис. Тогда модуль $S_\bullet(V) = V \otimes_C F$ изотипный типа F и разлагается в прямую сумму подмодулей $(v_\iota C) \otimes_C F$; каноническое отображение α_V: $V \to \mathscr{L}_A(F, V \otimes_C F)$ биективно. Для любого правого C-модуля V' отображение $f \to S(f)$ является биекцией множества $\mathscr{L}_C(V', V)$ на $\mathscr{L}_A(S(V'), S(V))$.*

б) *Обратно, пусть M — левый A-модуль, изотипный типа F, и $(u_\iota)_{\iota\in I}$ — семейство инъективных гомоморфизмов модуля F в M, таких, что M есть прямая сумма подмодулей $u_\iota(F)$. Тогда $T(M) = \mathscr{L}_A(F, M)$ — свободный правый C-модуль, семейство $(u_\iota)_{\iota\in I}$ — его базис и каноническое отображение β_M: $\mathscr{L}_A(F, M) \otimes_C F \to M$ биективно. Для любого левого A-модуля M' отображение $g \to T(g)$ является биекцией множества $\mathscr{L}_A(M, M')$ на $\mathscr{L}_C(T(M), T(M'))$.*

Сначала докажем лемму:

Лемма 2. *Пусть $(Q_\iota)_{\iota\in I}$ — семейство A-модулей, Q — их прямая сумма, P — A-модуль. Абелевы группы $\mathscr{L}_A(P, Q_\iota)$ отождествляются с некоторыми подгруппами в $\mathscr{L}_A(P, Q)$, порождающими их прямую сумму. Если, кроме того, модуль P конечного типа, то $\mathscr{L}_A(P, Q) = \Sigma_{\iota\in I}\, \mathscr{L}_A(P, Q_\iota)$.*

Первое утверждение немедленно следует из определений. Пусть модуль P порождается конечным семейством $(x_k)_{1\leqslant k\leqslant m}$ и $f \in \mathscr{L}_A(P, Q)$; для любого элемента x_k компоненты $f(x_k)$ в Q_ι все, кроме конечного числа, равны нулю. Следовательно, существует конечное подмножество J множества I, для которого $f(P) \subset \Sigma_{\iota\in J} Q_\iota$. Пусть $(P_\iota)_{\iota\in I}$ — семейство проектирований, ассоциированное с разложением $Q = \Sigma_{\iota\in J} Q_\iota$. Тогда $f = \Sigma_{\iota\in J} P_\iota \circ f$, откуда ввиду $p_\iota \circ f \in \mathscr{L}_A(P, Q_\iota)$ и следует лемма.

Докажем теперь обе части теоремы.

а) Отображения $x \to v_\iota \otimes x$ модуля F в V являются изоморфизмами модуля F на A-подмодули $(v_\iota C) \otimes_C F$ модуля $V \otimes_C F$, и $V \otimes_C F$ будет прямой суммой этих подмодулей (гл. III, приложение II, предложение 5). Пусть $v = \Sigma_{\iota \in I} v_\iota c_\iota$ $(c_\iota \in C)$ — элемент модуля V и $v \otimes x = 0$ для любого $x \in F$. Тогда $\Sigma_{\iota \in I} v_\iota \otimes (c_\iota x) = 0$, и следовательно, для любого индекса $\iota \in I$ равенство $c_\iota x = 0$ выполняется для всех $x \in F$, то есть, по определению C, $c_\iota = 0$; поэтому $v = 0$, то есть отображение α_V инъективно. По определению C, всякое A-линейное отображение модуля F в A-модуль, изоморфный $(v_\iota C) \otimes_C F$, имеет вид $x \to v_\iota \otimes c_\iota x = (v_\iota c_\iota) \otimes x$; лемма 2 показывает, что отображение α_V сюръективно и, следовательно, биективно.

Отсюда немедленно следует, что $f \to \alpha_V \circ f$ — биекция множества $\mathscr{L}_C(V', V)$ на $\mathscr{L}_C(V', \mathscr{L}_A(F, S(V)))$. Пусть σ — канонический изоморфизм группы $\mathscr{L}_C(V'; \mathscr{L}_A(F, S(V)))$ на $\mathscr{L}_A(V' \otimes_C F, S(V)) = \mathscr{L}_A(S(V), S(V'))$ (гл. III, приложение II, предложение 8). Покажем, что $\sigma(\alpha_V \circ f) = S(f)$; в самом деле, при $v' \in V'$ и $x \in F$ имеем $\sigma(\alpha_V \circ f)(v' \otimes x) = ((\alpha_V \circ f)(v'))(x) = (\alpha_V(f(v')))(x) = f(v') \otimes x = S(f)(v' \otimes x)$, откуда и следует наше утверждение

б) По предположению, из равенства $\sum_{\iota \in I} u_\iota \cdot c_\iota = 0$ $(c_\iota \in C)$ следует, что $u_\iota(c_\iota x) = 0$ для любого $x \in F$; так как гомоморфизм u_ι инъективен, то $c_\iota x = 0$, и следовательно, $c_\iota = 0$ по определению C; поэтому элементы u_ι линейно независимы в C-модуле $T(M)$. С другой стороны, всякое A-линейное отображение модуля F в A-модуль, изоморфный $u_\iota(F)$, имеет вид $u_\iota \cdot c_\iota$, $c_\iota \in C$ (по определению C); из леммы 2 следует, что система (u_ι) является базисом модуля $T(M)$. Всякий элемент модуля M является суммой элементов вида $u_\iota(x) = \beta_M(u_\iota \otimes x)$, $x \in F$, то есть отображение β_M сюръективно. С другой стороны, всякий элемент тензорного произведения $T(M) \otimes_C F$ может быть записан в виде $\sum_{\iota \in I} u_\iota \otimes x_\iota$, где элементы $x_s \in F$ все, кроме конечного числа, равны нулю; если этот элемент при отображении β_M имеет нулевой образ, то есть $\sum_{\iota \in I} u_\iota(x_\iota) = 0$, то $x_\iota = 0$ при любом ι; таким образом, отображение β_M инъективно и, следовательно, сюръективно.

Отсюда немедленно следует, что $g \to g \circ \beta_M$ — биекция множества $\mathscr{L}_A(M, M')$ на $\mathscr{L}_A(T(M) \otimes_C F, M')$. Пусть τ — канонический изоморфизм группы $\mathscr{L}_A(T(M) \otimes_C F, M')$ на $\mathscr{L}_C(T(M), \mathscr{L}_A(F, M')) = \mathscr{L}_C(T(M), T(M'))$ (гл. III, приложение II, предложение 8). Покажем, что $\tau(g \circ \beta_M) = T(g)$; в самом деле, при $u \in T(M)$ и $x \in F$ имеем $(g \circ \beta_M)(u \otimes x) = g(u(x))$, то есть $(\tau(g \circ \beta_M)(u))(x) = g(u(x))$; другими словами, $\tau(g \circ \beta_M)(u) = g \circ u = T(g)(u)$, что и заканчивает доказательство.

Следствие 1. *Если модуль F конечного типа и модуль V свободен, то отображение $f \to S(f)$ является изоморфизмом кольца $\mathscr{L}_C(V)$ на кольцо $\mathscr{L}_A(V \otimes_C F)$.*

Это следует из теоремы 1а) (взять $V = V$) и формул (3).

Следствие 2. *Если модуль F конечного типа и M — изотипный модуль типа F, то отображение $g \to T(g)$ является изоморфизмом кольца $\mathscr{L}_A(M)$ на кольцо $\mathscr{L}_C(\mathscr{L}_A(F, M))$.*

Это следует из теоремы 1б) (взять $M' = M$) и формул (5).

Если модуль M является прямой суммой *конечного* семейства n подмодулей, изоморфных F, то кольцо $\mathscr{L}_A(M)$ изоморфно кольцу $M_n(C)$ квадратных матриц порядка n над коммутантом C модуля F (гл. II. § 6, n° 5).

Следствие 3. *Пусть M — изотипный модуль типа F, $V = \mathscr{L}_A(F, M)$. Предположим, что модуль F конечного типа, и отождествим M с $V \otimes_C F$ с помощью β_M. Тогда формулы $M' = V' \otimes_C F$ и $V = \mathscr{L}_A(F, M')$ устанавливают взаимно однозначное соответствие между прямыми множителями V модуля V, являющимися свободными правыми C-модулями, и прямыми множителями M' модуля M, являющимися изотипными модулями типа F.*

Пусть e_1 — проектирование модуля V на V; тогда $S(e_1) = e_1 \otimes 1$ — проектирование модуля $V \otimes_C F$ на $V' \otimes_C F$. Аналогично, если e_2 — проектирование модуля M на M, то $T(e_2)\colon u \to e_2 \circ u$ — проектирование модуля $\mathscr{L}_A(F, M)$ на $\mathscr{L}_A(F, M')$. Отождествляя с помощью α_V (соответственно $\alpha_{V'}$) модули V (соответственно V') и $T(S(V))$ (соответственно $T(S(V'))$), ввиду теоремы 1 и формулы (6) получаем, что $e_1 = T(S(e_1))$; аналогично, отождествляя с помощью β_M (соответственно $\beta_{M'}$) модули M (соответственно M') и $S(T(M))$ (соответственно $S(T(M'))$), из формулы (7) получаем, что $e_2 = S(T(e_2))$, что и доказывает следствие.

З а м е ч а н и е. Теорема 1 и ее следствия, так же как и доказательство, остаются в силе, если не предполагать, что модуль F конечного типа, но ограничиваться модулями M с *конечным* базисом и изотипными модулями M, разлагающимися в прямую сумму *конечного* семейства подмодулей, изоморфных F. Тогда лемма 2 заменяется предложением 2 гл. II, § 2, n° 3.

У п р а ж н е н и я. 1) Пусть M — абелева группа, Ω — кольцо эндоморфизмов группы M.

а) Пусть p, q — проектирования в M; $p(M) \subset q(M)$ тогда и только тогда, когда $qp = p$; $p^{-1}(0) \subset q^{-1}(0)$ тогда и только тогда, когда $qp = q$.

б) Пусть $(p_i)_{1 \leqslant i \leqslant n}$ — конечное семейство проектирований в M и все $p_i(M)$ равны одной и той же подгруппе N группы M; пусть, далее, элементы a_i $(1 \leqslant i \leqslant n)$ кольца Ω удовлетворяют условиям $a_i p_j = p_j a_i$ для любых индексов i и j и $\sum_{i=1}^{n} a_i = 1$. Тогда $p = \sum_{i=1}^{n} a_i p_i$ — проектирование и $p(M) = N$.

в) Если p и q — проектирования такие, что $p + q$ — также проектирование, то $pq = -qp$, и обратно. Вывести отсюда, что если равенство $2x = 0$ влечет в группе M равенство $x = 0$, то $pq = 0$ (рассмотреть элемент $x \in p(M)$).

г) Пусть p и q — проектирования. Следующие условия эквивалентны: $\alpha)$ $pq = qp$; $\beta)$ $q(p(M)) \subset p(M)$ и $q(p^{-1}(0)) \subset p^{-1}(0)$, $\gamma)$ модуль M является прямой суммой четырех подмодулей N_1, N_2, N_3, N_4 таких, что $p(M) = N_1 + N_2$, $p^{-1}(0) = N_3 + N_4$, $q(M) = N_1 + N_3$, $q^{-1}(0) = N_2 + N_4$. При выполнении этих условий $r = pq$ и $s = p + q - pq$ являются проектированиями и справедливы равенства $r(M) = p(M) \cap q(M)$ и $s(M) = p(M) + q(M)$.

д) Пусть p — проектирование; подмодуль $p(M)$ устойчив относительно элемента $a \in \Omega$ тогда и только тогда, когда $pap = ap$.

е) Пусть p — проектирование в M, и $N = p(M)$. Предположим, что подмодуль N устойчив относительно любого элемента a некоторого подмножества A кольца Ω; пусть $\dot{a}$, $a \in A$, — эндоморфизм абелевой группы M/N, получаемый из эндоморфизма a путем факторизации; отображение $ap - pa$ в подмодуле N является нулевым и, следовательно, путем факторизации определяет некоторое отображение a_N модуля M/N в N. Подмодуль N имеет в M дополнение, устойчивое относительно любого $a \in A$, тогда и только тогда, когда существует гомоморфизм d абелевой группы M/N в абелеву группу N такой, что для любого $a \in A$ выполняется равенство $a_N = d\dot{a} - ad$.

2) Пусть M — абелева группа, Ω — кольцо ее эндоморфизмов, A — подкольцо в Ω, содержащее единичный элемент Ω, A' — коммутант и A'' — бикоммутант A в Ω.

а) Пусть A-модуль M является прямой суммой конечного семейства подмодулей $(N_i)_{1\leqslant i\leqslant n}$ и $(p_i)_{1\leqslant i\leqslant n}$ — семейство проектирований, ассоциированное с разложением $M = \sum_{i=1}^{n} N_i$. Показать, что кольцо A' есть прямая сумма правых идеалов p_iA' (соответственно левых идеалов $A'p_i$).

б) Обратно, пусть A' есть прямая сумма конечного семейства $(\mathfrak{r}_i)_{1\leqslant i\leqslant m}$ правых идеалов (соответственно конечного семейства $(\mathfrak{l}_i)_{1\leqslant i\leqslant m}$ левых идеалов); тогда A''-модуль M разлагается в прямую сумму некоторого семейства m подмодулей N_i $(1 \leqslant i \leqslant m)$, причем $\mathfrak{r}_i$ (соответственно $\mathfrak{l}_i$) есть множество таких элементов $u \in A'$, что $u(M) \subset N_i$ (соответственно $u(N_j) = \{0\}$ для любого $j \neq i$).

в) Пусть выполняются условия, указанные в а). Определить канонический изоморфизм абелевой группы $\mathscr{L}_A(N_i, N_j)$ на подгруппу $p_jA'p_i$ группы A'; показать, что при $j = i$ это отображение является изоморфизмом *колец*.

3) Пусть A — кольцо.

а) Для того чтобы элемент $e \in A$ был идемпотентом, необходимо и достаточно, чтобы отображение $x \to ex$ было проектированием в A-модуле A_s (или отображение $x \to xe$ было проектированием в A^0-модуле A_r).

б) Пусть e_1, e_2 — идемпотенты кольца A. Показать, что абелева группа $\mathscr{L}_A(Ae_1, Ae_2)$ изоморфна $(e_1A) \cap (Ae_2) = e_1Ae_2$, а кольцо $\mathscr{L}_A(Ae_1)$ изоморфно кольцу e_1Ae_1.

в) Пусть e_1, e_2 — идемпотенты кольца A. Показать, что следующие три условия эквивалентны: $\alpha)$ $Ae_1 = Ae_2$; $\beta)$ $e_1e_2 = e_1$ и $e_2e_1 = e_2$; $\gamma)$ $(1 - e_1)A = (1 - e_2)A$. Из этих условий следует, кроме того, что в кольце A существует обратимый элемент a такой, что $e_2 = ae_1a^{-1}$ (воспользоваться утверждением а) и упражнением 1а)).

г) Пусть e_1, e_2 — идемпотенты кольца A. Показать, что следующие три условия эквивалентны: $\alpha)$ левые A-модули Ae_1 и Ae_2 изоморфны; $\beta)$ правые A-модули e_1A и e_2A изоморфны; $\gamma)$ существуют элементы x, $y \in A$ такие, что $xy = e_2$, $yx = e_1$ (воспользоваться утверждением б)). При выполнении этих условий идемпотенты e_1 и e_2 называются *эквивалентными*.

д) Если идемпотенты e_1 и e_2 эквивалентны и принадлежат центру кольца A, то они равны.

е) Пусть $(e_i)_{1\leqslant i\leqslant n}$, $(f_i)_{1\leqslant i\leqslant n}$ — семейства n идемпотентов кольца A и для любых индексов i и j выполняются равенства $e_ie_j = \delta_{ij}e_j$, $f_if_j = \delta_{ij}f_j$. Показать, что если идемпотенты e_i и f_i при любом i, $1 \leqslant i \leqslant n$, эквивалентны, то $e = \sum_{i=1}^{n} e_i$ и $f = \sum_{i=1}^{n} f_i$ — эквивалентные идемпотенты.

4) Пусть M — векторное пространство размерности 3 над полем K, (e_1, e_2, e_3) — его базис над полем K и A — подкольцо в $\mathscr{L}_K(M)$, состоящее из эндоморфизмов, имеющих относительно базиса (e_1, e_2, e_3) матрицу вида

$$\begin{pmatrix} a & 0 & 0 \\ b & c & 0 \\ 0 & 0 & a \end{pmatrix}$$

(a, b, c — произвольные элементы поля K). Модуль M, рассматриваемый как A-модуль, является прямой суммой подмодулей $N = Ke_1 + Ke_2$ и $P = Ke_3$.

а) Показать, что бикоммутант B A-модуля M совпадает с A, каноническое отображение $b \to b_N$ бикоммутанта B в бикоммутант модуля N инъективно, но не сюръективно, а каноническое отображение $b \to b_P$ бикоммутанта B в бикоммутант модуля P сюръективно, но не инъективно.

б) Получить из а) пример модуля M' над кольцом A' и прямого множителя N' в M', для которых каноническое отображение бикоммутанта модуля M' в бикоммутант модуля N' не было ни инъективным, ни сюръективным (рассмотреть произведение $M' = M \times M$ как модуль над кольцом $A' = A \times A$).

5) Пусть A-модуль M — прямая сумма семейства $(F_\iota)_{\iota \in I}$ своих подмодулей, модуль F — один из F_ι, D — его бикоммутант. Предположим, что для любого индекса $\iota \in I$ существует A-изоморфизм модуля F_ι на D-подмодуль модуля F. Показать, что каноническое отображение $b \to b_F$ бикоммутанта модуля M в D сюръективно.

*6) Пусть K — поле, $A = K[X, Y]$ — кольцо многочленов от двух переменных над полем K, $\mathfrak{m}$ — идеал $(X) + (Y)$ кольца A, $\mathfrak{n}$ — идеал $(X^2) + (Y^2)$ кольца A, F — A-модуль $\mathfrak{m}/\mathfrak{n}$. Показать, что коммутант C модуля F изоморфен кольцу $A/\mathfrak{a}$, где $\mathfrak{a}$ — идеал $(X^2) + (XY) + (Y^2)$. Вывести отсюда, что в тензорном произведении $F \otimes_C F$ при любом $x \in F$ выполняется равенство $\varphi(XY) \otimes x = 0$ (φ — каноническое отображение модуля $\mathfrak{m}$ на $\mathfrak{m}/\mathfrak{n}$); вывести также, что каноническое отображение α_F модуля F в $T(S(F))$ не инъективно и не сюръективно.

7) а) Пусть в обозначениях упражнения 6 M — A-модуль $\mathfrak{m}/\mathfrak{a}$. Показать, что каноническое отображение β_M модуля $S(T(M))$ в M сюръективно, но не инъективно.

б) Привести пример кольца A и пары модулей A-модулей F, M таких, что отображение β_M модуля $S(T(M))$ в M инъективно, но не сюръективно (взять F и M таким образом, чтобы $\mathscr{L}_A(F, M) = \{0\}$).

в) Получить из а) и б) пример A-модулей F и M таких, что отображение β_M не инъективно и не сюръективно (так же, как в упражнении 4б)).

8) а) Пусть F — A-модуль, C — его коммутант, V — свободный правый C-модуль, $(v_\iota)_{\iota \in I}$ — базис модуля V. Показать, что коммутант

B A-модуля $M = V \otimes_C F$ изоморфен кольцу двойных семейств $(u_{\mu\lambda})_{(\mu,\lambda)\in I\times I}$ элементов C таких, что при любом $x \in F$ и любом $\lambda \in I$ элементы $u_{\mu\lambda}(x) = 0$ для всех μ, кроме конечного числа, а произведение $(s_{\mu\lambda})\,(t_{\mu\lambda}) = (u_{\mu\lambda})$ двух семейств определяется формулой

$$u_{\mu\lambda}(x) = \sum_{\nu\in I} s_{\mu\lambda}(t_{\nu\lambda}(x)).$$

Вывести отсюда, что отображение $f \to S(f)$ множества $\mathscr{L}_C(V)$ в $B = \mathscr{L}_A(M)$ инъективно; привести пример, в котором это отображение не сюръективно (в качестве A взять тело, и F — бесконечномерное векторное пространство над A).

б) Показать, что в контрмодуле модуля M (над B) всякий подмодуль имеет вид $V \otimes_C F'$, где F' — подмодуль контрмодуля модуля F.

в) Показать, что если множество I конечно и имеет n элементов, то кольцо B (изоморфное кольцу матриц $M_n(C)$) является прямой суммой n левых идеалов, изоморфных контрмодулю модуля M (см. упражнение 2а)).

9) Пусть кольцо A — прямая сумма конечного семейства левых идеалов $\mathfrak{l}_i$, изоморфных, как A-модули $(1 \leqslant i \leqslant n)$.

а) Показать, что в кольце A существует семейство элементов e_{ij} $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$ таких, что $e_{ij}e_{hk} = \delta_{jh}e_{ik}$ (δ_{jh} — символ Кронекера) и $\mathfrak{l}_i = Ae_{ii}$ (см. упражнение 3г) и гл. I, § 8, упражнение 15). Обратно, если в кольце A существует семейство n^2 элементов e_{ij} таких, что $e_{ij}e_{hk} = \delta_{jh}e_{ik}$ и $1 = e_{11} + e_{22} + \ldots + e_{nn}$, то левые идеалы Ae_{ii} изоморфны, как A-модули (см. упражнение 3г)). Пусть B — подкольцо в A, состоящее из элементов, перестановочных со всеми e_{ij}. Тогда кольцо A изоморфно кольцу матриц $M_n(B)$, а B изоморфно подкольцу, противоположному коммутанту каждого из A-модулей Ae_{ii} (применить предложение 4 и следствие 2 теоремы 1).

б) Пусть M — A-модуль. Показать, что $N_i = e_{ii}M$ являются B-модулями и M, рассматриваемый как B-модуль, есть прямая сумма модулей N_i $(1 \leqslant i \leqslant h)$; кроме того, B-модули N_i попарно изоморфны (рассмотреть отображения $x \to e_{i1}x$ и $y \to e_{1i}y$) и их аннулятор есть пересечение подкольца B и аннулятора M в кольце A. Обратно, для любого B-модуля N на прямой сумме M n B-модулей, изоморфных N, определить структуру A-модуля таким образом, чтобы $e_{11}M = N$.

в) Каждому B-подмодулю P модуля N_1 поставим в соответствие A-подмодуль $\sum_{i=1}^{n} e_{i1}P$ модуля M. Показать, что тем самым определено биективное отображение множества B-подмодулей модуля N_1 на множество A-подмодулей модуля M, строго возрастающее по включению.

§ 2. Артиновы и нетеровы модули

1. *Артиновы и нетеровы модули*

Определение 1. *Модуль M над кольцом A называется артиновым* (соответственно *нетеровым*), *если выполняются следующие эквивалентные условия*:

а) *всякое непустое множество подмодулей модуля M, упорядоченное по включению, имеет минимальный* (соответственно *максимальный*) *элемент*;

б) *всякая убывающая* (соответственно *возрастающая*) *последовательность подмодулей модуля M стационарна.*

Эквивалентность условий а) и б) следует из предложения 6, Теор. мн., гл. III, § 6, n° 5.

Для того чтобы модуль M был артиновым (соответственно нетеровым), необходимо и достаточно, чтобы он был артиновым (соответственно нетеровым) как модуль над своим кольцом гомотетий A_M.

Примеры. 1) Векторное пространство конечной размерности артиново и нетерово.

2) Пусть $(M_\iota)_{\iota \in I}$ — бесконечное семейство ненулевых модулей. Прямая сумма $M = \sum_{\iota \in I} M_\iota$ не является ни артиновым, ни нетеровым модулем: в самом деле, всякой бесконечной строго убывающей (соответственно строго возрастающей) последовательности (J_n) подмножества множества I соответствует бесконечная строго убывающая (соответственно строго возрастающая) последовательность подмодулей $P_n = \sum_{\iota \in J_n} M_\iota$ модуля M.

Лемма 1. *Пусть M — нетеров A-модуль, E — подмножество в M. В E существует конечное подмножество F, порождающее в M тот же подмодуль, что и E.*

В самом деле, пусть $\mathfrak{M}$ — множество подмодулей модуля M, порожденных конечными подмножествами из E, и N — максимальный элемент множества $\mathfrak{M}$. Тогда $N + Ax \in \mathfrak{M}$ при всяком $x \in N$, так что $N + Ax = N$, то есть $x \in N$. Отсюда $E \subset H$, что и доказывает лемму.

Предложение 1. *Для того чтобы A-модуль M был нетеровым, необходимо и достаточно, чтобы всякий его подмодуль был конечного типа.*

По лемме 1 это условие необходимо. Обратно, предположим, что оно выполнено. Пусть (P_n) — возрастающая последовательность подмодулей модуля M и P — объединение всех P_n. Подмодуль P порождается конечным числом элементов $x_1, \ldots, x_m$, следовательно, существует достаточно большое число n, такое, что все x_i принадлежат P_n, то есть $P_n = P$, откуда и следует, что M — нетеров модуль.

Предложение 2. *Для того чтобы A-модуль M был артиновым* (соответственно *нетеровым*), *необходимо и достаточно, чтобы существовал такой артинов* (соответственно *нетеров*) *подмодуль N, что фактормодуль M/N также артинов* (соответственно *нетеров*).

Если модуль M артинов (соответственно нетеров), то всякий его подмодуль N, очевидно, артинов (соответственно нетеров); фактормодуль M/N также артинов (соответственно нетеров): это следует из того, что отображение, ставящее в соответствие каждому подмодулю модуля M/N его обратный образ в M при каноническом отображении, инъективно и сохраняет включение (гл. I, § 6, n° 13, теорема 6). Обратно, предположим, что модули N и M/N артиновы (соответственно нетеровы). Пусть (P_n) — убывающая (соответственно возрастающая) последовательность подмодулей модуля M и (P'_n) — канонический образ подмодуля P_n в M/N. Последовательности $(P_n \cap N)$ и (P'_n) — убывающие (соответственно возрастающие) и, следовательно, стационарные; поэтому существует целое число i такое, что при $n \leqslant i$ выполняются равенства $P_n \cap N = P_i \cap N$ и $P'_n = P'_i$. Достаточно теперь доказать следующее утверждение: если подмодули F и G модуля M имеют одинаковые канонические образы в M/N, $F \subset G$ и $F \cap N = G \cap N$, то $F = G$. В самом деле, для всякого $x \in G$ существует $y \in F$ такой, что $x - y \in N$; отсюда $x - y \in G \cap N = F \cap N \subset F$, то есть $x \in F$.

Следствие. *Пусть модуль M есть прямая сумма конечного семейства подмодулей $(M_i)_{1 \leqslant i \leqslant n}$ и все M_i артиновы* (соответственно *нетеровы*). *Тогда модуль M артинов* (соответственно *нетеров*).

Достаточно рассмотреть случай $n = 2$ и применить индукцию по n. В этом случае модуль M/M_1 изоморфен $M_2/(M_1 \cap M_2)$ (гл. I, § 6, n° 13, теорема 6). Пользуясь предложением 2, можно последовательно убедиться, что модули $M_2/(M_1 \cap M_2)$ и M артиновы (соответственно нетеровы).

Модуль называется модулем *конечной длины*, если он обладает рядом Жордана — Гельдера (гл. I, § 6, n° 14).

Предложение 3. *Для того чтобы модуль M был конечной длины, необходимо и достаточно, чтобы он был одновременно и артиновым, и нетеровым.*

Если модуль M имеет конечную длину l, то всякая строго возрастающая (или строго убывающая) последовательность его подмодулей содержит не более $l + 1$ членов (гл. I, § 6, n° 14, следствие теоремы 8); следовательно, модуль M артинов и нетеров. Обратно, предположим, что модуль M нетеров, и пусть N — его подмодуль, отличный от $\{0\}$. Рассмотрим подмодуль P, максимальный среди подмодулей, содержащихся в N и отличных от N; модуль N/P, очевидно, прост (как группа с операторами) (гл. I, § 6, n° 13, теорема 6). Применяя последовательно этот результат, построим строго убывающую (конечную или бесконечную) последовательность (M_n) подмодулей модуля M, в которой $M_0 = M$ и все факторы M_i/M_{i+1} просты. Если теперь модуль M артинов, то эта последовательность конечна и является, следовательно, рядом Жордана — Гельдера.

2. *Разложение модуля конечной длины на неразложимые модули*

Лемма 2. *Пусть u — эндоморфизм модуля M, L_p — образ эндоморфизма u^p, N_p — ядро u^p (p — целое > 0).*

а) *Если $L_1 = L_2$, то $N_1 + L_1 = M$. Если $N_1 = N_2$, то $N_1 \cap L_1 = \{0\}$.*

б) *Если модуль M артинов* (соответственно *нетеров*), *то для достаточно большого r выполняется равенство $N_r + L_r = M$* (соответственно $N_r \cap L_r = \{0\}$).

Пусть $L_1 = L_2$; для любого элемента $x \in M$ существует $y \in M$ такой, что $u(x) = u^2(y)$; тогда $x - u(y) \in N_1$ и $x = (x - u(y)) + u(y) \in N_1 + L_1$.

Пусть $N_1 = N_2$; для всякого $x \in N_1 \cap L_1$ имеем равенство $u(x) = 0$, и существует $y \in M$ такой, что $x = u(y)$; тогда $y \in N_2 = N_1$, откуда $x = u(y) = 0$.

Если модуль M артинов (соответственно нетеров), то при r достаточно большом $L_r = L_{2r}$ (соответственно $N_r = N_{2r}$), откуда, по предыдущему, $N_r + L_r = M$ (соответственно $N_r \cap L_r = \{0\}$).

Лемма 3. *Пусть M — артинов* (соответственно *нетеров*) *модуль, u — его эндоморфизм. Для того чтобы u был биективен, необходимо и достаточно, чтобы он был инъективен* (соответственно *сюръективен*).

Если модуль M артинов (соответственно нетеров) и эндоморфизм u инъективен (соответственно сюръективен), то, в обозначениях леммы 2, $L_r = M$ (соответственно $N_r = \{0\}$) при r достаточно большом. Следовательно, $L_1 = M$ (соответственно $N_1 = \{0\}$).

Предложение 4. *Пусть M — неразложимый A-модуль конечной длины, не сводящийся к 0* (гл. VII, § 4, n° 7, определение 3). *Необратимые эндоморфизмы модуля M нильпотентны и образуют двусторонний идеал в кольце $\mathscr{L}_A(M)$.*

Если эндоморфизм $u \in \mathscr{L}_A(M)$ не имеет обратного, то по лемме 3 он не инъективен и не сюръективен; так как модуль M неразложим, то ввиду леммы 2 отсюда следует, что M совпадает с ядром некоторой степени u^r, другими словами, эндоморфизм u нильпотентен. С другой стороны, эндоморфизмы uv и vu необратимы при любом $v \in \mathscr{L}_A(M)$. Наконец, если эндоморфизмы v и w необратимы, то $u = v + w$ необратим; в самом деле, в противоположном случае мы бы имели равенство $1 = v' + w'$, где $v' = u^{-1}v$, $w' = u^{-1}w$ — необратимые и, следовательно, нильпотентные эндоморфизмы; однако v' и $w' = 1 - v'$ перестановочны, так что соотношения $v'^n = 0$ и $w'^n = 0$, справедливые для достаточно большого n, по формуле бинома влекут равенство $1 = (v' + w')^{2n-1} = 0$, что явно неверно.

Теорема 1. *Пусть M — модуль конечной длины.*

а) *Модуль M разлагается в прямую сумму конечного семейства $(M_i)_{1 \leqslant i \leqslant m}$ неразложимых подмодулей, не сводящихся к 0.*

б) *Если модуль M является прямой суммой другого семейства $(M'_j)_{1\leqslant j\leqslant n}$ неразложимых подмодулей, не сводящихся к 0, то $m = n$, и существуют перестановка π интервала $[1, n]$ и автоморфизм α модуля M такие, что $\alpha(M'_j) = M_{\pi(j)}$, $1 \leqslant j \leqslant n$.*

Утверждение а) доказывается индукцией по длине модуля M: всякий модуль длины 1 неразложим, а если модуль M разложим, то он является прямой суммой двух подмодулей, длины которых строго меньше, чем длина модуля M.

Докажем утверждение б). Пусть $(p_i)_{1\leqslant i\leqslant m}$, $(p'_j)_{1\leqslant j\leqslant n}$ — два семейства проектирований, ассоциированных с разложениями $M = \sum_{i=1}^{m} M_i$ и $M = \sum_{j=1}^{n} M'_j$. Индукцией по r для любого $r \in [0, n]$ докажем следующее утверждение:

(A_r) при $1 \leqslant j \leqslant r$ существуют такая инъекция π_r интервала $[1, r]$ в $[1, m]$ и такой автоморфизм α_r модуля M, что $\alpha_r(M'_j) = M_{\pi_r(j)}$.

При $r = 0$ за автоморфизм α_0 можно принять тождественный автоморфизм модуля M. Предположим, что уже получены инъекция π_{r-1} и автоморфизм α_{r-1}, удовлетворяющие условию (A_{r-1}). Очевидно, что, заменяя каждый подмодуль M'_j на $\alpha_{r-1}(M'_j)$ и меняя при необходимости нумерацию подмодулей M'_j, можно считать теперь, что $M'_i = M_j$, $1 \leqslant j \leqslant r-1$.

Сужение на подмодуль M'_r отображения $p'_r = \sum_{i=1}^{m} p'_r p_i$ является тождественным автоморфизмом M'_r. Следовательно (предложение 4), сужения на M'_r эндоморфизмов $p'_r p_i$ не могут все содержаться в идеале необратимых эндоморфизмов модуля M'_r; иными словами, существует число $k \in [1, m]$, для которого сужение на M'_r отображения $p'_r p_k$ является автоморфизмом модуля M'_r. При $1 \leqslant j \leqslant r-1$ имеем $p_j = p'_j p_j$, откуда $p'_r p_j = (p'_r p'_j)\, p_j = 0$; следовательно, $k \geqslant r$. Положив $\pi_r(j) = j$ для $1 \leqslant j \leqslant r-1$ и $\pi_r(r) = k$, определим инъекцию π_r. Положим еще $\alpha_r = 1 - p'_r + p_k p'_r$. Отображение α_r инъективно: если $\alpha_r(x) = 0$, то $0 = p'_r \alpha_r(x) = (p'_r p_k)(p'_r(x))$, так что $p'_r(x) = 0$, и следовательно, $x = \alpha_r(x) + p'_r(x) - p_k p'_r(x) = 0$. По лемме 3 α_r — автоморфизм модуля M. Ясно, что α_r индуцирует на M'_j, $j \neq r$, тождественное отображение и $\alpha_r(M_r) \subset M_k$. Отсюда следует, что модуль M_k разлагается

в прямую сумму $\alpha_r(M'_r)$ и $M_k \cap (\sum_{j \neq r} \alpha_r(M'_j))$. Но M_k неразложим, так что $\alpha_r(M'_r) = M_k$, что доказывает (A_r) и заканчивает, следовательно, доказательство теоремы 1.

3. *Артиновы и нетеровы кольца*

Определение 2. *Кольцо A называется артиновым слева* (соответственно *справа*), *если модуль A_s* (соответственно A_r) *артинов. Кольцо A называется нетеровым слева* (соответственно *справа*), *если модуль A_s* (соответственно A_r) *нетеров.*

Таким образом, кольцо A артиново (соответственно нетерово) слева, если всякая убывающая (соответственно возрастающая) последовательность его левых идеалов обрывается. Кольцо нетерово слева, если всякий его левый идеал имеет конечную систему образующих (предложение 1).

В случаях, когда будет идти речь об артиновом (соответственно нетеровом) кольце без уточнения, будет подразумеваться, что оно артиново (соответственно нетерово) слева.

Примеры. 1) Пусть A — кольцо и D — подтело в A, содержащее его единицу. Если кольцо A конечномерно как векторное пространство над D, то A артиново и нетерово. В частности, всякая алгебра конечной размерности над некоторым полем является артиновым и нетеровым кольцом слева и справа.

2) Кольцо главных идеалов (гл. VII, § 1, n° 1) нетерово, так как всякий его идеал порождается одним элементом. Например, кольцо Z нетерово. Однако кольцо Z не артиново, так как при $a > 1$ последовательность идеалов (a^n) возрастает и не стационарна.

3) Если модуль A_s (соответственно A_r) конечной длины, то кольцо A артиново слева (соответственно справа); длина модуля A_s (соответственно A_r) называется *левой длиной* (соответственно *правой длиной*) кольца A (если A коммутативно, то просто *длиной* A). Мы увидим (§ 6, n° 5, следствие 3 предложения 12), что всякое артиново кольцо является нетеровым и, следовательно, имеет конечную длину (n° 1, предложение 3) (см. в упражнении 1б) пример артинова, но не нетерова модуля).

4) Пусть $(M_\iota)_{\iota \in I}$ — бесконечное семейство модулей, не сводящихся к 0, M — их прямая сумма. Кольцо L эндоморфизмов

модуля M не является ни артиновым, ни нетеровым. В самом деле, пусть $\mathfrak{l}_\iota$, $\iota \in I$,— левый идеал кольца L, состоящий из элементов $c \in L$, таких, что $c\,(M_\varkappa) \neq \{0\}$ при $\varkappa \neq \iota$. Идеалы $\mathfrak{l}_\iota$ образуют бесконечное семейство подмодулей модуля L_s, и сумма их прямая, откуда и следует наше утверждение (см. n° 1, пример 2).

Из предложения 2 немедленно получаются следующие результаты.

Предложение 5. *Произведение конечного числа артиновых* (соответственно *нетеровых*) *колец— артиново* (соответственно *нетерово*) *кольцо.*

Предложение 6. *Факторкольцо артинова* (соответственно *нетерова*) *кольца по двустороннему идеалу — артиново* (соответственно *нетерово*) *кольцо.*

Напротив, подкольцо артинова (соответственно нетерова) кольца не обязано быть артиновым (соответственно нетеровым) кольцом.

Пусть, например, K — поле. Кольцо $K\,[X_n]_{n\in N}$ многочленов от бесконечного множества переменных с коэффициентами из поля K является кольцом целостности (гл. IV, § 1, n° 4, теорема 1) и содержится, следовательно, в своем поле дробей. Но это кольцо не является ни артиновым, так как последовательность идеалов $(X_0^m)_{m\geqslant 1}$ строго убывает, ни нетеровым, так как последовательность идеалов $a_n = (X_0) + (X_1) + \ldots + (X_n)$ строго возрастает.

Предложение 7. *Всякий левый модуль конечного типа над кольцом, артиновым* (соответственно *нетеровым*) *слева, артинов* (соответственно *нетеров*).

В самом деле, если A-модуль M имеет систему из n образующих, то он изоморфен фактормодулю произведения A_s^n (гл. II, § 1, n° 8, предложение 10).

Мы увидим (§ 6, n° 5, следствие 1 предложения 12), что фактически всякий модуль конечного типа над артиновым кольцом имеет конечную длину.

Лемма 4. *Пусть M — точный A-модуль* (гл. II, § 1, n° 9) *и $(x_\iota)_{\iota\in I}$ — семейство образующих его контрмодуля. Тогда отображение $a \to (ax_\iota)_{\iota\in I}$ является A-изоморфизмом модуля A_s на некоторый подмодуль в M^I.*

Очевидно, это отображение является A-гомоморфизмом модуля A_s в M^I, и достаточно доказать, что оно инъективно. Пусть

$ax_\iota = 0$ при всех $\iota \in I$. Тогда для всякого семейства $(c_\iota)_{\iota \in I}$ элементов кольца $\mathscr{L}_A(M)$, всех, кроме конечного числа, равных нулю, имеем равенство $a(\sum_{\iota \in I} c_\iota x_\iota) = \sum_{\iota \in I} c_\iota (ax_\iota) = 0$; таким образом, $a \cdot M = \{0\}$, и следовательно, $a = 0$, так как модуль M точный.

Предложение 8. *Пусть M — артинов* (соответственно *нетеров*) *A-модуль. Если его контрмодуль конечного типа, то кольцо гомотетий A_M артиново* (соответственно *нетерово*).

Так как модуль M — артинов (соответственно нетеров) A_M-модуль, то доказательство сводится к случаю, когда модуль M точный. По лемме 4 существует целое число n такое, что A_s изоморфен некоторому подмодулю в M^n. Достаточно теперь применить предложение 2 и его следствие.

Следствие. *Пусть M — нетеров A-модуль. Если кольцо A коммутативно, то кольцо A_M нетерово.*

Модуль M конечного типа (предложение 1), так что его контрмодуль в силу $A_M \subset \mathscr{L}_A(M)$ также конечного типа.

Упражнения. 1) а) Привести пример нетерова, но не артинова модуля M, у которого всякий ненулевой эндоморфизм инъективен и существуют ненулевые небиективные эндоморфизмы.

б) Привести пример артинова, но не нетерова модуля M, у которого всякий эндоморфизм $\neq 0$ сюръективен и существуют ненулевые небиективные эндоморфизмы (взять в качестве M модуль U_Π (гл. VII, § 2, упражнение 3)).

2) Пусть M, N — A-модули конечной длины и существует целое число n такое, что M^n и N^n изоморфны. Показать, что M и N изоморфны (воспользоваться теоремой 1).

3) Пусть M — модуль конечной длины n, R — подмножество кольца $\mathscr{L}(M)$ эндоморфизмов модуля M, устойчивое относительно умножения, и всякий элемент его нильпотентен.

а) Показать, что если $n = 1$, то $R = \{0\}$. В случае $n > 1$ и $R \neq \{0\}$ показать, что в M имеется подмодуль N, устойчивый относительно всех элементов множества R и отличный от $\{0\}$ и от M. (Среди всех ненулевых элементов множества R рассмотреть элемент s, для которого модуль $s(M)$ имеет наименьшую возможную длину; рассуждая от противного, показать, что $srs = 0$ для всех $r \in R$. Вывести отсюда, что при $Rs = \{0\}$ в качестве N можно взять $s(M)$, а в противоположном случае — прямую сумму подмодулей $rs(M)$ (где $r \in R$) *).)

б) Вывести из а), что модуль M обладает рядом Жордана — Гельдера $M = M_0 \supset M_1 \supset \ldots \supset M_n = \{0\}$ таким, что $r(M_i) \subset$

*) Это доказательство (неопубликованное) сообщил нам А. Розенберг.

$\subset M_{i+1}$ при $0 \leqslant i \leqslant n-1$ (провести индукцию по n). В частности, если $(r_i)_{1 \leqslant i \leqslant n}$ — произвольная последовательность n элементов множества R, то $r_1 r_2 \ldots r_n = 0$.

4) а) Пусть K — поле и φ — его изоморфизм на такое его подполе K', что K, рассматриваемое как векторное пространство над K', бесконечномерно (гл. V, § 6, упражнение 1). На аддитивной группе $A = K \times K$ с помощью формулы

$$(x, y)(x', y') = (xx', xy' + y\varphi(x'))$$

определим структуру кольца с единицей. Показать, что единственным левым идеалом кольца A, отличным от A к $\{0\}$, будет $\{0\} \times K$ в то же время всякое произведение $\{0\} \times E$, где E — некоторое векторное подпространство в V, является правым идеалом кольца A. Вывести отсюда, что кольцо A артиново слева, но не артиново и не нетерово справа (см. § 6, упражнение 25).

б) Привести пример модуля конечной длины, кольцо эндоморфизмов которого не является ни артиновым, ни нетеровым слева (использовать а)).

в) С помощью метода из упражнения а) привести пример кольца A, артинова и нетерова слева и справа, у которого модули A_s и A_d имеют различную длину.

5) Пусть A — кольцо, $e \in A$ — идемпотент.

а) Пусть $\mathfrak{l}_1$ — левый идеал в кольце eAe, и $\mathfrak{l}$ — левый идеал, порожденный идеалом $\mathfrak{l}_1$ в кольце A. Показать, что $\mathfrak{l}_1 = e\mathfrak{l}e = \mathfrak{l} \cap eAe$.

б) Показать, что для любого левого идеала $\mathfrak{l}$ кольца A справедливо включение $\mathfrak{l} \cap (eAe) \subset e\mathfrak{l}e$; привести пример, в котором эти два идеала кольца A различны (рассмотреть кольцо матриц).

в) Показать, что для всякого двустороннего идеала $\mathfrak{a}$ кольца A справедливо равенство $e\mathfrak{a}e = \mathfrak{a} \cap eAe$.

г) Вывести из а), что если кольцо A артиново (соответственно нетерово), то и кольца eAe и $(1-e)A(1-e)$ артиновы (соответственно нетеровы).

д) Показать, что кольцо матриц $M_n(B)$ над кольцом B артиново (соответственно нетерово) тогда и только тогда, когда артиново (соответственно нетерово) кольцо B (можно использовать упражнение 9в) § 1).

6) Пусть A и B — кольца, M — множество, наделенное структурой левого A-модуля и правого B-модуля, причем $a(xb) = (ax)b$, $a \in A$, $x \in M$, $b \in B$. Показать, что формула $(x, y, z)(x', y', z') = (xx', xy' + yz', zz')$ определяет на произведении $C = A \times M \times B$ структуру кольца; в кольце C элементы $e = (1, 0, 0)$ и $e' = (0, 0, 1)$ являются идемпотентами, элемент $e + e'$ — единицей. Привести пример, в котором A и B — тела, но кольцо C не артиново и не нетерово (см. упражнение 5г)).

7) а) Пусть A — кольцо, $\mathcal{J}$ — множество левых идеалов вида Ae, где e — идемпотент. Показать, что четыре следующих условия эквивалентны:

α) всякое подмножество в $\mathcal{J}$ имеет минимальный элемент;

β) всякое подмножество в $\mathcal{J}$ имеет максимальный элемент;

γ) не существует бесконечного семейства идеалов, принадлежащих $\mathcal{J}$ и составляющих прямую сумму;

δ) в кольце A не существует бесконечного семейства ортогональных идемпотентов.

б) Показать, что в кольце A^0, противоположном кольцу A, определенному в упражнении 4, всякое множество *моногенных* левых идеалов имеет максимальный и минимальный элементы, так что условия упражнения а) тем более выполняются для кольца A^0 (см. § 6, упражнение 30).

в) Показать, что если в модуле E всякое множество подмодулей конечного типа имеет максимальный элемент, то E — нетеров модуль.

8) а) Пусть A — кольцо, u, v — элементы кольца A, $uv = 1$, $vu \neq 1$. Положим $e_{ij} = v^{i-1}u^{j-1} - v^iu^j$, $i \geqslant 1$, $j \geqslant 1$; показать, что $e_{ij} \neq 0$ и $e_{ij}e_{hk} = \delta_{jh}e_{ik}$. Вывести отсюда, что в кольце A существует левый идеал, являющийся прямой суммой счетного множества изоморфных левых идеалов (см. § 1, упражнение 3г)). Показать, что при любом $j > 1$ имеет место равенство $u(v + e_{1j}) = 1$ и при $j \neq k$ $e_{1j} \neq e_{1k}$.

б) Пусть кольцо A удовлетворяет условиям упражнения 7а) и $uv = 1$, u, $v \in A$. Вывести из а), что $vu = 1$ (см. § 5, упражнение 12).

9) Пусть A — кольцо и B — подкольцо в A, содержащее его единицу. Показать, что если кольцо A артиново (соответственно нетерово) справа и как левый B-модуль имеет базис над B, то и подкольцо B артиново (рассмотреть пересечения множеств Ba_ι, где $(a_\iota)_{\iota \in I}$ — базис модуля A над B, с правым идеалом кольца A, порожденным правым идеалом $\mathfrak{r}$ кольца B). Справедливо ли обратное утверждение, хотя бы в случае, когда A (как B-модуль) имеет конечный базис (см. упражнение 4)?

10) Пусть A — кольцо, B и D — его подкольца. Показать, что если кольцо B артиново, а D — тело, то $B \cap D$ — тело (для любого $x \in B \cap D$ рассмотреть последовательность идеалов Bx^n кольца B).

11) Пусть A — артиново (соответственно нетерово) слева кольцо, M и N — дополнительные подмодули левого A-модуля A_s^n. Показать, что если A-модуль M свободен, то модуль N также свободен (использовать теорему 1 n° 2).

12) Пусть A — кольцо, $\mathfrak{a}$ и $\mathfrak{b}$ — его двусторонние идеалы, и кольца $A/\mathfrak{a}$ и $A/\mathfrak{b}$ нетеровы (соответственно артиновы). Показать, что кольцо $A/(\mathfrak{a} \cap \mathfrak{b})$ нетерово (соответственно артиново) (использовать предложение 2).

§ 3. Простые и полупростые модули

1. *Простые модули*

Определение 1. *Модуль M называется простым, если он не сводится к 0 и не имеет подмодулей, отличных от M и $\{0\}$.*

Простой модуль, рассматриваемый как группа с операторами, является простой группой с операторами (гл. I, § 6, n° 14, определение 14).

Для того чтобы модуль M над кольцом A был простым, необходимо и достаточно, чтобы он был простым как модуль над кольцом A_M гомотетий.

Предложение 1. *Пусть M — A-модуль, отличный от $\{0\}$. Модуль M прост тогда и только тогда, когда $M = Ax$ для любого его элемента $x \neq 0$.*

В самом деле, если $x \neq 0$, то Ax является подмодулем в M, отличным от $\{0\}$.

Следствие. *Всякий простой модуль моногенен.*

Предложение 2. *Пусть A — кольцо, $\mathfrak{m}$ — его левый идеал. Для того чтобы A-модуль $A_s/\mathfrak{m}$ был прост, необходимо и достаточно, чтобы $\mathfrak{m}$ был максимальным левым идеалом кольца A.*

В самом деле, подмодули модуля $A_s/\mathfrak{m}$ являются каноническими образами левых идеалов $\mathfrak{n}$ кольца A, содержащих $\mathfrak{m}$ (гл. I, § 8, n° 9, теорема 5).

Предложение 3. *Пусть M — простой A-модуль. Для любого элемента $x \neq 0$ модуля M аннулятор $\mathfrak{m}$ этого элемента является максимальным левым идеалом кольца A. Отображение $\alpha \to \alpha x$ кольца A на M определяет путем факторизации A-изоморфизм модуля $A_s/\mathfrak{m}$ на M.*

Элемент x является образующим модуля M (предложение 1), и поэтому второе утверждение справедливо. Первое утверждение следует из второго и предложения 2.

Примеры простых модулей. 1) Пусть A — кольцо. Простые подмодули модуля A_s являются минимальными элементами упорядоченного по включению множества левых

идеалов $\neq \{0\}$ кольца A; они называются *минимальными левыми идеалами* кольца A. Аналогично определяются минимальные правые идеалы и минимальные двусторонние идеалы. Как показывает пример кольца $A = Z$, такие идеалы существуют не всегда.

2) Пусть D — тело, V — векторное пространство над D, A — подкольцо, порожденное в $\mathscr{L}_D(V)$ единицей (тождественным автоморфизмом пространства V) и эндоморфизмами пространства V, имеющими *конечный* ранг. Тогда V является простым A-модулем и тем более простым модулем над кольцом $\mathscr{L}_D(V)$. В самом деле, любой ненулевой элемент $x \in V$ можно рассматривать как элемент некоторого базиса B пространства V (гл. II, § 3, n° 1, теорема 2); для любого $z \in V$ существует эндоморфизм $u \in \mathscr{L}_D(V)$ такой, что $u(x) = z$ и $u(y) = 0$ для всех $y \in B$, $y \neq x$; очевидно, $u \in A$, и наше утверждение следует из предложения 1. Пусть x' — линейная форма $\neq 0$ на V и u_x, $x \in V$,— эндоморфизм $y \to < y, x' > x$ пространства V; равенство $v \circ u_x = u_{v(x)}$ справедливо, очевидно, для любого $v \in \mathscr{L}_D(V)$; следовательно, отображение $x \to u_x$ является гомоморфизмом $\mathscr{L}_D(V)$-модуля V на некоторый левый идеал кольца $\mathscr{L}_D(V)$; этот идеал, будучи фактормодулем модуля V, отличным от 0, *минимален*.

3) Пусть A — кольцо. Модуль A_s прост тогда и только тогда, когда $\{0\}$ является единственным левым идеалом кольца A, отличным от A, то есть если A — тело (гл. I, § 9, n° 3, предложение 3). В этом случае всякий простой A-модуль изоморфен A_s (предложение 3).

4) Пусть A — кольцо главных идеалов. Простыми A-модулями будут A-модули $A_s/(p)$, где p — экстремальный элемент кольца A (предложения 2 и 3). Если $n > 1$, то модуль $A_s/(p^n)$ неразложимый (гл. VII, § 4, n° 7, предложение 6), но не простой.

Определение 2. *Пусть M — модуль. Максимальным подмодулем модуля M называется всякий максимальный элемент упорядоченного по включению множества подмодулей M, отличных от M. Иными словами, максимальным называется всякий подмодуль N, для которого модуль M/N прост.*

Предложение 4. *Пусть M — модуль конечного типа, и L — его отличный от M подмодуль. Существует максимальный подмодуль модуля M, содержащий L.*

Достаточно показать, что множество $\mathfrak{M}$ подмодулей модуля M, отличных от M, индуктивно (Теор. мн., Рез., § 6, n° 10); пусть $\mathfrak{G}$ — подмножество в $\mathfrak{M}$, совершенно упорядоченное по включению; надо показать, что подмодуль Q — объединение подмодулей $P \in \mathfrak{G}$ — отличен от M. Пусть F — конечное подмножество в M, порождающее M. Если $Q = M$, то каждый элемент из F принадлежит некоторому подмодулю $P \in \mathfrak{G}$, то есть F содержится в одном из этих подмодулей, что противоречит предположению.

Следствие. *Пусть M — A-модуль конечного типа, отличный от $\{0\}$. В кольце A существует двусторонний идеал $\mathfrak{a}$, аннулирующий некоторый простой A-модуль и такой, что $\mathfrak{a} \cdot M \neq M$.*

В самом деле, в модуле M имеется максимальный подмодуль N (предложение 4). Пусть $\mathfrak{a}$ — аннулятор простого A-модуля M/N; из равенства $\mathfrak{a} \cdot M/N = \{0\}$ следует $\mathfrak{a} \cdot M \subset N$.

Предложение 5. *Пусть A — кольцо, $\mathfrak{l}$ — его минимальный левый идеал, M — точный простой A-модуль. Тогда M изоморфен A-модулю $\mathfrak{l}$.*

Пусть $\alpha \neq 0$ — элемент $\mathfrak{l}$. Существует $x \in M$ такой, что $\alpha x \neq 0$. Пусть $\mathfrak{m}$ — аннулятор элемента x, то есть максимальный левый идеал (предложение 3). Тогда $\alpha \notin \mathfrak{m}$, так что $\mathfrak{m} \cap \mathfrak{l} \neq \mathfrak{l}$. Но идеал $\mathfrak{l}$ минимален, и отсюда следует, что $\mathfrak{m} \cap \mathfrak{l} = \{0\}$. Так как идеал $\mathfrak{m}$ максимален, то $A_s = \mathfrak{m} + \mathfrak{l}$. Таким образом, модуль A_s является прямой суммой подмодулей $\mathfrak{l}$ и $\mathfrak{m}$, и следовательно, M, будучи изоморфным $A_s/\mathfrak{m}$, изоморфен $\mathfrak{l}$.

Предложение 6. *Пусть M — точный A-модуль, обладающий рядом Жордана — Гельдера Σ. Если его контрмодуль конечного типа, то всякий простой A-модуль изоморфен одному из факторов ряда Σ.*

Всякий простой A-модуль изоморфен простому фактормодулю модуля A_s (предложение 3). По лемме 4 § 2, n° 3, A_s изоморфен подмодулю модуля M^n, n — некоторое целое число. Следовательно, всякий простой A-модуль изоморфен некоторому фактору ряда Жордана — Гельдера модуля M^n (гл. I, § 6, n° 14, следствие теоремы 8). Однако ясно, что модуль M^n обладает рядом Жордана — Гельдера, факторы которого изоморфны факторам ряда Σ.

2. Классы простых модулей

Обозначим через $Is_A(X, Y)$ отношение «A — кольцо, и X, Y — изоморфные простые A-модули». Это отношение является отношением эквивалентности между X и Y. Если X и Y — простые изоморфные A-модули, то истинно соотношение $(\forall Z)(Is_A(X, Z) \Leftrightarrow Is_A(Y, Z))$. Но схема S7 (Теор. мн.; гл. I, § 5, n° 1) дает следующую аксиому:

$$((\forall Z)\ (Is_A(X,Z) \Leftrightarrow Is_A(Y,Z))) \Rightarrow (\tau_Z(Is_A(X,Z)) = \tau_Z(Is_A(Y,Z))).$$

Следовательно, если X и Y — изоморфные простые A-модули, то

$$\tau_Z(Is_A(X, Z)) = \tau_Z(Is_A(Y, Z)).$$

Если X — простой A-модуль, то $\tau_Z(Is_A(X, Z))$ называется *классом A-модуля X*; говорят также, что X-модуль класса $\tau_Z(Is_A(X, Z))$. Так как отношение $Is_A(X, X)$ истинно, класс модуля X является простым A-модулем, изоморфным X. Таким образом, два простых модуля изоморфны тогда и только тогда, когда они одного класса.

Отношение «λ — класс простых A-модулей» является *коллективизирующим* по λ (Теор. мн., гл. II, § 1, n° 4). В самом деле, пусть $\mathfrak{Q}_A$ — множество простых A-модулей — фактормодулей модуля A_s (подмножество в $\mathfrak{P}(\mathfrak{P}(A))$ и $\mathfrak{S}_A$ — множество объектов вида $\tau_Z(Is_A(X, Z))$, $X \in \mathfrak{Q}_A$ (Теор. мн., гл. II, § 1, n° 6). По предложению 3 $\lambda \in \mathfrak{Q}_A$ для любого класса λ простых A-модулей. $\mathfrak{S}_A$ называется *множеством классов простых A-модулей*.

3. Полупростые модули

Теорема 1. *Пусть модуль M — сумма (не обязательно прямая) семейства $(N_\iota)_{\iota \in I}$ простых подмодулей. Для любого подмодуля F модуля M существует подмножество $J \subset I$ такое, что M является прямой суммой F и семейства $(N_\iota)_{\iota \in J}$.*

Пусть $\mathfrak{S}$ — множество подмножеств $L \subset I$, для которых сумма $F + \sum_{\iota \in L} N_\iota$ — прямая. Множество $\mathfrak{S}$ конечного характера и имеет, следовательно, максимальный элемент J (Теор. мн., § 6, n° 11). Пусть $V = F + \sum_{\iota \in J} N_\iota$ и $\iota \in I$; сумма $V + N_\iota$ не прямая, так как множество J максимально. Поэтому $N_\iota \cap V \neq \{0\}$, то есть $N_\iota \subset V$,

так как модуль N_i прост. Следовательно, $M = V$, что и доказывает теорему.

Предложение 7. *Пусть M — модуль. Следующие свойства эквивалентны:*

а) *M — сумма семейства простых подмодулей;*

б) *M — прямая сумма семейства простых подмодулей;*

в) *всякий подмодуль модуля M является прямым слагаемым*

Теорема 1, примененная к $F = \{0\}$, показывает, что из а) следует б); если подмодуль F произвольный, то по теореме 1 из б) следует в). Наконец, предположим, что модуль M обладает свойством в). Пусть $F \neq \{0\}$ — моногенный подмодуль в M. По предложению 4 в F имеется подмодуль N такой, что модуль F/N прост. Пусть N' — дополнение подмодуля N в M; подмодуль $N' \cap F$ является дополнением подмодуля N в F и изоморфен F/N, то есть прост. Тем самым доказано, что всякий подмодуль $\neq \{0\}$ модуля M содержит простой подмодуль.

Обозначим тогда через P сумму простых подмодулей модуля M и через P' — дополнение P в M. Тогда $P' = \{0\}$, так как в противном случае модуль P' содержал бы простой подмодуль и пересечение $P \cap P'$ было бы отлично от $\{0\}$, что неверно. Это и заканчивает доказательство.

Определение 3. *Модуль M называется полупростым, если он удовлетворяет эквивалентным условиям из предложения 7.*

A-модуль M полупрост тогда и только тогда, когда он полупрост как модуль над кольцом A_M гомотетий.

Всякий модуль, являющийся прямой суммой некоторого семейства полупростых подмодулей, полупрост.

Примеры полупростых модулей. 1) Модуль, сводящийся к 0, полупрост.

2) Всякий простой модуль полупрост.

3) Если A — тело, то всякий моногенный A-модуль, не сводящийся к 0, изоморфен A_s и, следовательно, прост; поэтому всякий A-модуль полупрост. Таким образом, мы снова получаем свойства векторных пространств (гл. II, § 3, теорема 1 и предложение 5).

4) Группа $\boldsymbol{Z}$ как $\boldsymbol{Z}$-модуль не является полупростым $\boldsymbol{Z}$-модулем: она не имеет ненулевых конечных подмодулей, а всякий простой $\boldsymbol{Z}$-модуль конечен (n° 1, пример 4).

Предложение 8. *Пусть модуль M — сумма некоторого семейства $(N_\iota)_{\iota\in I}$ простых подмодулей. Для всякого его подмодуля N* (соответственно *для всякого его фактормодуля N*) *существует подмножество $J \subset I$ такое, что сумма $\sum_{\iota\in J} N_\iota$ прямая и изоморфна N.*

Так как в модуле M каждый подмодуль обладает дополнением (предложение 7), то всякий подмодуль изоморфен некоторому фактормодулю модуля M. Поэтому достаточно доказать предложение в случае, когда N есть фактормодуль модуля M по некоторому подмодулю P. Ввиду теоремы 1 в этом случае существует такое подмножество $J \subset I$, что сумма $N' = \sum_{\iota\in J} N_\iota$ — прямая и является дополнением подмодуля P в M; тогда модуль $N = M/P$ изоморфен N'.

Следствие 1. *Всякий подмодуль и всякий фактормодуль полупростого модуля полупросты.*

Следствие 2. *Пусть модуль M — прямая сумма семейства $(N_\iota)_{\iota\in I}$ простых подмодулей. Всякий простой подмодуль модуля M изоморфен одному из N_ι.*

4. *Изотипные компоненты полупростых модулей*

Пусть M — A-модуль, S — простой A-модуль. Сумма N подмодулей модуля M, изоморфных S, является полупростым подмодулем в M и прямой суммой некоторых подмодулей, изоморфных S (теорема 1); следовательно, модуль N — изотипный типа S. Модуль N называется *изотипной компонентой модуля M* типа S.

Предложение 9. *Пусть M — полупростой A-модуль, $\mathfrak{S}$ — множество классов простых A-модулей и M_λ, $\lambda \in \mathfrak{S}$, — изотипная компонента модуля M типа λ.*

а) *Модуль M — прямая сумма компонент M_λ.*

б) *Всякий подмодуль N модуля M является прямой суммой пересечений $N \cap M_\lambda$.*

В самом деле, пусть $\lambda \in \mathfrak{S}$, $\mathfrak{S}' = \mathfrak{S} - \{\lambda\}$ и $M'_\lambda = \sum_{\mu \in \mathfrak{S}'} M_\mu$. Всякий простой подмодуль модуля $M_\lambda \cap M'_\lambda$ должен быть одновременно класса λ и класса $\neq \lambda$ (следствие 2 предложения 8); поэтому $M_\lambda \cap M'_\lambda = \{0\}$, откуда следует, что сумма $\sum_{\lambda \in \mathfrak{S}} M_\lambda$ — прямая. Так как модуль M полупрост, то, очевидно, $M = \sum_{\lambda \in \mathfrak{S}} M_\lambda$; отсюда следует а). Так как модуль N полупрост (следствие 1 предложения 8), то он является суммой своих изотипных компонент N_λ; но, по определению, $N_\lambda \subset N \cap M_\lambda$, а с другой стороны, ввиду предложения 8, $N \cap M_\lambda \subset N_\lambda$, что и доказывает б).

Замечание. Сумма

$$\sum_{\lambda \in \mathfrak{S}} M_\lambda$$

будет прямой без всяких предположений об A-модуле M.

Предложение 10. *Пусть M, N — A-модули, f — гомоморфизм модуля M в N, λ — класс простых A-модулей, N_λ и N_λ — изотипные компоненты типа λ модулей M и N. Тогда $f(M_\lambda) \subset N_\lambda$.*

В самом деле, образ $f(M_\lambda)$ изоморфен фактормодулю компоненты M_λ и, следовательно, изотипен типа λ (предложение 8).

Предложение 11. *Пусть M — полупростой A-модуль, N — его подмодуль. Для того чтобы подмодуль N был устойчив относительно всех эндоморфизмов модуля M, необходимо и достаточно, чтобы N был прямой суммой некоторого семейства изотипных компонент модуля M.*

Вследствие предложения 10 это условие достаточно. Обратно, предположим, что подмодуль N устойчив относительно всех эндоморфизмов модуля M. Пусть S — простой подмодуль в N класса λ. Для любого простого подмодуля S' модуля M класса λ существует эндоморфизм c модуля M такой, что $c(S) = S'$: достаточно взять композицию изоморфизма модуля S на S' и проектирования модуля M на S (предложение 7). Таким образом, по предположению, $S' \subset N$; следовательно, изотипная компонента типа λ модуля M содержится в N, что и заканчивает доказательство.

5. *Длина полупростых модулей*

Теорема 2. *Пусть M — полупростой A-модуль, $(N_\alpha)_{\alpha\in I}$ и $(N'_\beta)_{\beta\in J}$ — два семейства простых подмодулей модуля M и M является одновременно прямой суммой подмодулей N_α и подмодулей N'_β. Тогда множества I и J равномощны.*

Если I или J конечно, то они равномощны по теореме 8 и следствию теоремы 8 гл. I, § 6, n° 14. Предположим теперь, что множества I и J бесконечны. Пусть x_α — элемент N_α такой, что $N_\alpha = Ax_\alpha$, и $C(\alpha)$ — конечное множество индексов $\beta \in J$, для которых компонента x_α в N'_β (относительно разложения $M = \sum_{\beta\in J} N'_\beta$) отлична от нуля; положим $C = \bigcup_{\alpha\in I} C(\alpha)$. Имеем $\mathrm{Card}\,(C) \leqslant \mathrm{Card}\,(I)$ (Теор. мн., гл. III, § 6, n° 3, следствие 3 теоремы 2). Однако при всяком $\alpha \in I$ $x_\alpha \in \sum_{\beta\in C} N'_\beta$, то есть $N_\alpha \subset \sum_{\beta\in C} N'_\beta$; следовательно, $M = \sum_{\beta\in C} N'_\beta$, откуда $C = J$. Значит, $\mathrm{Card}\,(J) \leqslant \mathrm{Card}\,(I)$, и точно так же доказывается, что $\mathrm{Card}\,(I) \leqslant \mathrm{Card}\,(J)$, то есть $\mathrm{Card}\,(I) = \mathrm{Card}\,(J)$.

Определение 4. *Пусть M — полупростой A-модуль. Длиной модуля M называется кардинальное число любого множества его простых подмодулей, прямая сумма которых равна M; длина модуля M обозначается через $l_A(M)$. Через $[M : F]$, где F — простой A-модуль, обозначается длина изотипной компоненты модуля M типа F.*

Длина модуля M равна $l_A(M) = \sum_{\lambda\in\mathfrak{S}} [M: \lambda]$, где $\mathfrak{S}$ — множество классов простых A-модулей.

Замечания. 1) Пусть M — полупростой A-модуль. Утверждение, что длина $l_A(M)$ конечна, равносильно утверждению, что модуль M имеет конечную длину в смысле § 2, n° 1, и в этом случае его длина $l_A(M)$ совпадает с длиной в смысле гл. I, § 6, n° 14.

2) Пусть M — векторное пространство над телом D. Утверждение, что длина $l_D(M)$ конечна, равносильно утверждению, что пространство M конечномерно, и в этом случае $l_D(M) = \dim_D(M)$. Для любого векторного пространства M над телом D *определим* раз-

мерность $\dim_D(M)$, положив $\dim_D(M) = l_D(M)$. Таким образом, эта размерность является кардинальным числом любого базиса пространства M.

Предложение 12. *Пусть M и N — полупростые A-модули. Для того чтобы модули M и N были изоморфны, необходимо и достаточно, чтобы для любого класса λ простых A-модулей изотипные компоненты типа λ модулей M и N имели одинаковую длину.*

Предложение очевидно.

Предложение 13. *Для того чтобы полупростой модуль имел конечную длину, необходимо и достаточно, чтобы он был конечного типа.*

Пусть $M = \sum_{\iota \in I} M_\iota$ — разложение модуля M в прямую сумму простых подмодулей. Все модули M_ι моногенны; поэтому, если множество I конечно, то модуль M конечного типа. Обратно, пусть $(x_j)_{1 \leqslant j \leqslant n}$ — конечная система образующих модуля M; каждый элемент x_j содержится в сумме некоторого конечного числа модулей M_ι, следовательно, множество I конечно.

Упражнения. 1) Пусть V — векторное пространство над телом D, V^* — сопряженное пространство, $A = \mathscr{L}_D(V)$ — кольцо эндоморфизмов пространства V. Закон композиции $(u, x') \to {}^t u(x')$ $(u \in A,\ x' \in V^*)$ определяет на V^* структуру правого A-модуля; пусть B — подкольцо, порожденное в A единичным элементом и эндоморфизмами конечного ранга; показать, что модуль V^* прост как A-модуль и как B-модуль.

2) Пусть A — кольцо.

а) Пусть M_1, M_2 — моногенные A-модули. Показать, что следующие условия эквивалентны: α) M_1 и M_2 изоморфны; β) для любого образующего x_1 модуля M_1 существует образующий x_2 модуля M_2, имеющий тот же аннулятор, что и x_1; γ) существуют образующий x_1 модуля M_1 и образующий x_2 модуля M_2, имеющие одинаковый аннулятор.

б) Пусть $\mathfrak{l}_1$, $\mathfrak{l}_2$ — левые идеалы кольца A. Для того чтобы A-модули $A/\mathfrak{l}_1$ и $A/\mathfrak{l}_2$ были изоморфны, необходимо и достаточно, чтобы в A существовал элемент α со следующими свойствами: 1° $A\alpha + \mathfrak{l}_2 = A$; 2° условия $\xi \in \mathfrak{l}_1$ и $\xi\alpha \in \mathfrak{l}_2$ эквивалентны (использовать а)).

в) Пусть $\mathfrak{m}_1$, $\mathfrak{m}_2$ — максимальные левые идеалы кольца A. Для того чтобы простые A-модули $A_s/\mathfrak{m}_1$ и $A_s/\mathfrak{m}_2$ были изоморфны, необходимо и достаточно, чтобы в кольце A существовал элемент α, не принадлежащий $\mathfrak{m}_2$ и такой, что $\mathfrak{m}_1\alpha \subset \mathfrak{m}_2$.

г) Вывести из б), что кардинальное число множества фактормодулей модуля A_s, изоморфных данному фактормодулю $A_s/\mathfrak{l}$, не превосходит Card (A).

3) Пусть M — A-модуль такой, что для любого элемента $x \in M$, отличного от 0, A-модуль Ax прост. Показать, что либо модуль M прост, либо кольцо гомотетий A_M — тело (если M не прост, рассмотреть ненулевые элементы x, $y \in M$ такие, что $y \notin Ax$ и аннулятор их суммы $x + y$).

4) Для того чтобы модуль M был полупростым, необходимо и достаточно, чтобы для любого его подмодуля N, отличного от M, в M существовал подмодуль $P \neq \{0\}$ такой, что $N \cap P = \{0\}$.

5) а) Пусть M — A-модуль и аннулятор элемента $x \in M$ является пересечением конечного семейства $(\mathfrak{m}_i)_{1 \leqslant i \leqslant n}$ максимальных левых идеалов. Показать, что подмодуль A^x полупрост (погрузить A^x в произведение модулей $A_s/\mathfrak{m}_i$).

б) Вывести из а), что A-модуль M полупрост тогда и только тогда, когда аннулятор всякого ненулевого элемента $x \in M$ является пересечением конечного семейства максимальных левых идеалов кольца A.

6) Пусть M — модуль. Показать, что следующие три условия эквивалентны:

α) M — полупростой модуль конечной длины;

β) M — нетеров модуль, и всякий его максимальный подмодуль обладает дополнением;

γ) M — артинов модуль, и всякий его простой подмодуль обладает дополнением.

7) Пусть K — тело, I — бесконечное множество, A — произведение K^I, показать, что в A-модуле A_s всякий *моногенный* подмодуль обладает дополнением, однако модуль A_s не полупрост (описать простые подмодули в A_s) (см. § 6, упражнение 15).

8) Показать, что $\boldsymbol{Z}$-модуль $\boldsymbol{Q}$ не имеет ни простых подмодулей, ни простых фактормодулей.

9) Пусть M — модуль.

а) Пусть u — нильпотентный эндоморфизм модуля; показать, что $1 + u$ — автоморфизм модуля M.

б) Пусть $M = \sum_\iota M_\iota$ — разложение модуля M в прямую сумму подмодулей. Показать, что существуют эндоморфизм u модуля M и различные индексы α и β такие, что $u(M_\alpha) \subset M_\beta$ и $u(M_\alpha) \neq \{0\}$, и существует автоморфизм v модуля M такой, что $v(M_\alpha) \not\subset M_\alpha$ и $v(M_\lambda) = M_\lambda$ для всех $\lambda \neq \alpha$ (использовать а)). Доказать обратное утверждение.

10) Пусть M — модуль конечной длины, и $M = \sum_{i=1}^{n} N_i$ — его разложение в прямую сумму неразложимых подмодулей (§ 2,

теорема 1); пусть (J_k) — разбиение отрезка $[1, n]$ на классы эквивалентности чисел i и j по отношению «N_i и N_j изоморфны», и P_k — изотипный модуль, являющийся прямой суммой подмодулей N_i, $i \in J_k$. Показать на примере, что подмодули P_k не обязательно устойчивы относительно автоморфизмов модуля M (взяв в качестве M Z-модуль конечной длины, применить упражнение 9).

11) Пусть A — кольцо, и A-модули A_s и A_d имеют конечную длину; отождествим модуль A_d с сопряженным модулем к A_s. Для всякого левого идеала $\mathfrak{l}$ (соответственно всякого правого идеала $\mathfrak{r}$) ортогональный к нему в A_d (соответственно в A_s) идеал $\mathfrak{l}^0$ (соответственно $\mathfrak{r}^0$) является правым аннулятором идеала $\mathfrak{l}$ (соответственно левым аннулятором идеала $\mathfrak{r}$) в A. Будем рассматривать следующие свойства кольца A:

α_s) Для любого простого левого A-модуля сопряженный модуль прост или сводится к 0.

α_d) Для любого простого правого A-модуля сопряженный модуль прост или сводится к 0.

β_s) Для любого минимального левого идеала $\mathfrak{l}$ $\mathfrak{l}^{00} = \mathfrak{l}$.

β_d) Для любого правого минимального идеала $\mathfrak{r}$ $\mathfrak{r}^{00} = \mathfrak{r}$.

γ) Длины модулей A_s и A_d равны.

а) Показать, что из условия β_d) следует α_s). Если условие α_s) выполнено, то длина модуля E^*, сопряженного к левому A-модулю E конечной длины, не превосходит этой длины (заметить, что для любого подмодуля M модуля E фактормодуль E^*/M^0 изоморфен некоторому подмодулю сопряженного к M модуля M^*; провести индукцию по длине модуля E).

б) Показать, что любые два из условий α_s), α_d) и γ) влекут третье (использовать а) и тот факт, что всякий левый A-модуль конечной длины изоморфен некоторому фактормодулю модуля A_s^n). При выполнении этих условий кольцо A называется *инволютивным*. В этом случае для любого левого или правого A-модуля E конечной длины длины модуля E и его сопряженного E^* равны и модуль E^* отождествляется с E; для любого подмодуля M в E выполняется равенство $M^{00} = M$, и его сопряженный модуль изоморфен E^*/M^0; кроме того, для любых двух подмодулей M и N модуля E имеем $(M \cap N)^0 = M^0 + N^0$.

12) Подмодуль M модуля E называется *накрытым*, если в фактормодуле E/M существует простой подмодуль. Модуль E называется *полуартиновым*, если всякий его подмодуль, отличный от E, накрытый. Всякий артинов модуль полуартинов. Всякое векторное пространство полуартиново.

а) Пусть E — модуль, F — его подмодуль, отличный от E. Для того чтобы модуль E был полуартинов, необходимо и достаточно, чтобы модули F и E/F были полуартиновы. (Для доказательства того, что если модуль E полуартинов, то и модуль F полуартинов, рассмотреть максимальный элемент в множестве подмодулей M модуля E таких, что $M \cap F = \{0\}$.)

б) Если модуль E является прямой суммой некоторого семейства полуартиновых подмодулей, то и E полуартинов.

в) Пусть K — тело, A — кольцо K^N. Показать, что A-модуль A_s является произведением простых A-модулей, но не полуартинов. (Рассмотреть в кольце A прямую сумму S минимальных левых идеалов и показать, что A-модуль A_s/S не содержит простых A-модулей.)

г) Показать, что если кольцо A нетерово, то всякий полуартинов A-модуль является прямой суммой артиновых подмодулей.

д) Пусть E — векторное пространство бесконечной размерности, A — подкольцо, порожденное в $\mathscr{L}(E)$ эндоморфизмами конечного ранга и единицей. Показать, что A-модуль A_s полуартинов (использовать а) и б)), но не является суммой своих артиновых подмодулей (см. § 5, упражнение 3).

§ 4. Коммутант и бикоммутант полупростого модуля

1. *Бикоммутант полупростого модуля*

Пусть M — полупростой A-модуль, B — его бикоммутант. Очевидно, всякий B-подмодуль модуля M является его A-подмодулем. Обратно, всякий A-подмодуль модуля M является прямым слагаемым (§ 3, n° 3, предложение 7) и, следовательно, (§ 1, n° 3, предложение 5а)) B-подмодулем.

С другой стороны, пусть N_1 и N_2 — подмодули модуля M. N_1 и N_2 A-изоморфны тогда и только тогда, когда они B-изоморфны (§ 1, n° 3, предложение 5в)).

Из предыдущего следует, что справедливо утверждение а) в следующем предложении:

Предложение 1. *Пусть M — полупростой A-модуль, B — его бикоммутант.*

а) *Для того чтобы модуль M был простым* (соответственно *изотипным полупростым*) *A-модулем, необходимо и достаточно, чтобы он был простым* (соответственно *изотипным полупростым*) *B-модулем.*

б) *Пусть $(M_\lambda)_{\lambda \in \mathfrak{S}}$ — семейство изотипных компонент модуля M и b_λ, $b \in B$, — сужение b на M_λ. Отображение $b \to (b_\lambda)$ является тогда изоморфизмом кольца B на произведение бикоммутантов компонент M_λ.*

в) *Если M — изотипный полупростой модуль и S — его простой подмодуль, то канонический гомоморфизм $b \to b_S$ кольца B в бикоммутант B_S модуля S является изоморфизмом B на B_S.*

Утверждение в) является частным случаем предложения 8 § 1, n° 3. Остается доказать б). Ясно, что отображение $b \to (b_\lambda)$ является инъективным гомоморфизмом кольца B в произведение бикоммутантов компонент M_λ. С другой стороны, пусть c_λ, $\lambda \in \mathfrak{S}$, — элемент бикоммутанта модуля M_λ. Существует единственный Z-эндоморфизм c модуля M, сужение которого на любой M_λ совпадает с c_λ. Достаточно показать, что $c \in B$. Подмодули M_λ устойчивы относительно любого эндоморфизма $d \in \mathscr{L}_A(M)$ (§ 3, n° 4, предложение 10), следовательно, сужение d_λ эндоморфизма d на M_λ принадлежит $\mathscr{L}_A(M_\lambda)$. По предположению, d_λ и c_λ перестановочны при любом $\lambda \in \mathfrak{S}$, так что эндоморфизмы d и c перестановочны, что и заканчивает доказательство.

2. *Теорема плотности*

Лемма 1. *Пусть M — полупростой A-модуль, b — элемент бикоммутанта B модуля M и $x \in M$. Существует элемент $a \in A$ такой, что $ax = bx$.*

В самом деле, A-подмодуль Ax является B-подмодулем (n° 1), так что $bx \in Ax$.

Теорема 1 (теорема плотности). *Пусть M — полупростой A-модуль, и b — элемент бикоммутанта B модуля M. Для любой конечной последовательности $(x_i)_{1 \leqslant i \leqslant n}$ элементов модуля M существует элемент $a \in A$ такой, что $ax_i = bx_i$ для всех $1 \leqslant i \leqslant n$.*

Пусть f_i, $i \in [1, n]$,— канонический изоморфизм модуля M на i-й множитель модуля M^n. Вследствие предложения 8 § 1, n° 3, в бикоммутанте модуля M^n найдется элемент b' такой, что $b'f_i = f_i b$, $1 \leqslant i \leqslant n$. Применив лемму 1 к элементу $x = (x_i) = \sum_{i=1}^{n} f_i(x_i)$ модуля M^n, получим, что существует элемент $a \in A$ такой, что

$$ax = b'x = \sum_{i=1}^{n} b' f_i(x_i) = \sum_{i=1}^{n} f_i(bx_i),$$

откуда следует равенство $ax_i = bx_i$, $1 \leqslant i \leqslant n$.

Следствие 1. *Пусть M — полупростой A-модуль. Если его контрмодуль является модулем конечного типа, то бикоммутант B модуля M совпадает с его кольцом гомотетий A_M.*

Пусть $b \in B$. Нужно доказать, что существует элемент $a \in A$ такой, что $b = a_M$. Пусть M' — контрмодуль модуля M, и F — конечная система его образующих. По теореме 1 в кольце A существует элемент a такой, что b и a_M совпадают на множестве F; но тогда $b = a_M$, так как b и a_M являются эндоморфизмами модуля M'.

Следствие 2. *Пусть $M_1, M_2, \ldots, M_n$ — простые A-модули различных классов, и предположим, что контрмодули их — конечного типа. Пусть $a_1, a_2, \ldots, a_n$ — элементы кольца A. В кольце A существует элемент a такой, что*

$$a_{M_i} = (a_i)_{M_i}, \quad 1 \leqslant i \leqslant n.$$

В самом деле, пусть M — прямая сумма модулей M_i. A-модуль M полупрост, и его изотипными компонентами являются M_i. Следовательно, семейство $(a_i)_{M_i}$ определяет элемент b бикоммутанта A-модуля M (предложение 1). С другой стороны, контрмодуль модуля M — конечного типа (всякий эндоморфизм одного из модулей M_i может быть продолжен до эндоморфизма модуля M). По следствию 1 в кольце A найдется элемент a такой, что $a_M = b$, что и доказывает следствие.

Пусть L — кольцо эндоморфизмов абелевой группы E, и A и B — подкольца в L. Подкольцо A называется *плотным* относительно B, если для всякой конечной последовательности $(x_i)_{1 \leqslant i \leqslant n}$ элементов E и всякого элемента $b \in B$ существует $a \in A$ такой, что

$$ax_i = bx_i, \quad 1 \leqslant i \leqslant n.$$

°Если в группу E введена дискретная топология, а в кольцо L — топология простой сходимости (Общ. топол., Рез., § 13, n° 2), то это свойство выражает тот факт, что A плотно относительно B в топологии пространства L.° Теорема 1 может быть выражена тогда следующим образом: если A-модуль M полупрост, то его кольцо гомотетий плотно в своем бикоммутанте.

°Заметим, что пространство L отделимо и умножение в L непрерывно. Следовательно, коммутант всякого подмножества замкнут в L, так же, как и его бикоммутант. Следовательно, бикоммутантом полупростого модуля E является замыкание в L кольца его гомотетий.°

3. *Коммутант простого модуля*

Лемма 2. *Пусть M и N — A-модули, и f — ненулевой гомоморфизм модуля M в N. Если модуль M прост, то f инъективен; если модуль N прост, то f сюръективен. Если модули M и N просты, то f биективен.*

В самом деле, образ гомоморфизма f является ненулевым подмодулем в N, а ядро — подмодулем в M, отличным от M. Это доказывает два первых утверждения. Третье утверждение следует из двух первых.

Предложение 2 (лемма Шура). *Коммутант простого модуля является телом.*

В самом деле, по лемме 2 всякий ненулевой элемент этого коммутанта обратим.

Таким образом, контрмодуль простого A-модуля M является *векторным пространством* над коммутантом D модуля M, и размерность его над D не обязательно конечна; бикоммутант модуля M является кольцом эндоморфизмом $\mathscr{L}_D(M)$ этого векторного пространства, и кольцо гомотетий модуля M плотно в $\mathscr{L}_D(M)$ (теорема 1).

Следствие (теорема Бернсайда). *Пусть A — алгебра над* алгебраически замкнутым *полем K и M — простой A-модуль конечной размерности над K. Тогда $A_M = \mathscr{L}_K(M)$, и коммутант модуля M есть поле K_M гомотетий α_M, где α пробегает K.*

В самом деле, коммутант D модуля M является телом (предложение 2), содержащимся в $\mathscr{L}_K(M)$ и содержащим в своем центре поле K_M. Покажем, что $D = K_M$, чем ввиду следствия теоремы 1 и закончится доказательство. Кольцо $\mathscr{L}_K(M)$, а следовательно и D, имеет конечный ранг над полем K_M (гл. II, § 7, n° 6); следовательно, и D имеет конечный ранг над K_M. Поэтому следствие вытекает из леммы:

Лемма 3. *Пусть K — алгебраически замкнутое поле, D — его надтело, имеющее над K конечную размерность и содержащее его в своем центре; тогда $D = K$.*

В самом деле, пусть $x \in D$. Подтело $K(x)$ тела D, порожденное элементом x, является коммутативным расширением конечного ранга над K и, следовательно, совпадает с K. Отсюда $x \in K$.

Следствие 2. *Пусть A — алгебра над алгебраически замкнутым полем K, и $M_1, M_2, \ldots, M_n$ — простые A-модули различных классов, конечномерные над K. Пусть $c_i \in \mathscr{L}_K(M_i)$, $1 \leqslant i \leqslant n$; существует элемент $a \in A$ такой, что $a_{M_i} = c_i$, $1 \leqslant i \leqslant n$.*

Это вытекает из предыдущего следствия и следствия 2 теоремы плотности (теорема 1).

Предложение 3. *Пусть M — полупростой A-модуль, S — простой A-модуль, D — коммутант модуля S. Абелевы группы $\mathscr{L}_A(S, M)$ и $\mathscr{L}_A(M, S)$ наделяются каноническими структурами соответственно правого и левого векторного D-пространства* (гл. III, приложение II, n° 7). *Тогда $[M : S] = \dim {}_D\mathscr{L}_A(S, M)$; кроме того, существует единственный изоморфизм T пространства $\mathscr{L}_A(M, S)$ на пространство, двойственное к $\mathscr{L}_A(S, M)$, такой, что для любых элементов $u \in \mathscr{L}_A(S, M)$, $v \in \mathscr{L}_A(M, S)$ имеет место равенство $\langle T(v), u \rangle = v \circ u$.*

Пусть N — изотипная компонента модуля M типа S. Вследствие предложения 10 § 3 векторные D-пространства $\mathscr{L}_A(S, M)$ и $\mathscr{L}_A(M, S)$ канонически отождествляются с $\mathscr{L}_A(S, N)$ и $\mathscr{L}_A(N, S)$. С другой стороны, $[M : S] = [N : S]$. Поэтому можно считать в дальнейшем, что модуль M — изотипный типа S. Поскольку модуль S моногенный (и, следовательно, конечного типа), то по теореме 1б) § 1, n° 5, $[M : S] = \dim {}_D\mathscr{L}_A(S, M)$. Кроме того, эта теорема показывает, что определенное в § 1, n° 4, отображение $v \to T(v)$ пространства $\mathscr{L}_A(M, S)$ в $\mathscr{L}_D(\mathscr{L}_A(S, M), \mathscr{L}_A(S, S)) = \mathscr{L}_D(\mathscr{L}_A(S, M), D)$ биективно. Однако модуль $\mathscr{L}_D(\mathscr{L}_A(S, M), D)$, по определению, двойствен к $\mathscr{L}_A(S, M)$, так что при $u \in \mathscr{L}_A(S, M)$, $v \in \mathscr{L}_A(M, S)$, по определению, имеем равенство $T(v)(u) = v \circ u$; следовательно, отображение $v \to T(v)$ линейно относительно структур левых векторных D-пространств; так как единственность отображения T очевидна, доказательство предложения 3 закончено.

Следствие. *Если выполняются условия предложения* 3, *то длина* $[M : S]$ *конечна тогда и только тогда, когда конечна* $\dim_D \mathscr{L}_A(M, S)$. *Тогда* $[M : S] = \dim \mathscr{L}_A(M, S)$.

Это следует из предложения 3 и свойств двойственного векторного пространства (гл. III, § 4, n° 4).

4. *Коммутант полупростого модуля*

Теперь мы в два приема сведем изучение коммутанта полупростого модуля к изучению коммутанта простого модуля.

Предложение 4. *Пусть* S *— простой* A*-модуль,* D *— его коммутант,* M *— изотипный полупростой* A*-модуль типа* S, $C = \mathscr{L}_A(M)$ *— его коммутант. Наделим* $T = \mathscr{L}_A(S, M)$ *каноническими структурами правого векторного* D*-пространства и левого* C*-модуля* (гл. III, приложение II, n° 7).

а) *Канонический гомоморфизм* (§ 1, n° 4, 2)) *кольца* C *в кольцо* $\mathscr{L}_D(T)$ *биективен.* C*-модуль* T *прост, и его коммутант изоморфен телу* D^0, *противоположному* D.

б) *Каноническое отображение* (§ 1, n° 4, 3)) *модуля* $T \otimes_D S$ *в* M *является изоморфизмом* $T \otimes_D S$ *на* M *для структур* A*-модуля и* C*-модуля.*

в) *Контрмодуль модуля* M *полупрост и изотипен типа* T (T *рассматривается как* C*-модуль). Верны равенства* $l_A(M) = \dim_D(T)$, $l_C(M) = \dim_D(S)$ (S *и* T *рассматриваются как левое и правое векторное* D*-пространство соответственно*).

Так как S — моногенный A-модуль, то первое утверждение в а) является частным случаем следствия 2 теоремы 1 § 1, n° 5. D — тело, так что T, рассматриваемый как левый модуль над кольцом $\mathscr{L}_D(T)$, прост (§ 3, n° 1, пример 2), и его коммутант есть кольцо гомотетий правого векторного D-пространства T (§ 1, n° 3, предложение 6), то есть изоморфен D^0; отсюда следуют остальные утверждения в а). В том, что касается структур A-модуля, утверждение б) является частным случаем теоремы 1б) § 1, n° 5; формула (7) § 1, n° 4 показывает, что канонический гомоморфизм тензорного произведения $T \otimes S$ в M является также и гомоморфизмом C-модулей D. Равенство $l_A(M) = \dim_D(T)$ следует из теоремы 1а) § 1, n° 5. Наконец, рассмотрим S (соответственно T) как правое (соответственно левое) векторное простран-

ство над D^0. Тогда $T \otimes_D S$ отождествляется с $S \otimes_{D^0} T$ (гл. III, приложение II, n° 9, предложение 9), D^0 является коммутантом моногенного C-модуля T и S — свободный правый D^0-модуль. Следовательно, применив к $S \otimes_{D^0} T$ теорему 1а) § 1, n° 5, получим остальные утверждения в в).

Следствие. *Формулы* $M' = T' \otimes_D S$ *и* $T' = \mathscr{L}_A(S, M')$ *устанавливают взаимно однозначное соответствие между векторными подпространствами* T' *пространства* T *и подмодулями* M' *модуля* M.

Всякое векторное подпространство T' пространства T является прямым слагаемым и имеет базис над телом D. Всякий подмодуль M' модуля M является прямым слагаемым и изотипен типа S (§ 3, n° 3, предложения 7 и 8). Поэтому следствие вытекает из следствия теоремы § 1, n° 5.

Предложение 5. *Пусть* $M = \sum_{\lambda \in \mathfrak{S}} M_\lambda$ *— разложение полупростого* A*-модуля в прямую сумму его изотипных компонент* M_λ, *и* C *— коммутант модуля* M.

а) *Пусть* c_λ, $c \in C$,— *сужение* c *на* M_λ. *Тогда отображение* $c \to (c_\lambda)_{\lambda \in \mathfrak{S}}$ *является изоморфизмом кольца* C *на произведение коммутантов компонент* M_λ.

б) *Модуль* M, *рассматриваемый как* C*-модуль, полупрост, и* M_λ *являются его изотипными компонентами.*

Утверждение а) сразу следует из предложения 10 § 3, n° 4. С другой стороны, по предложению 4 каждая компонента M_λ является изотипным полупростым модулем над кольцом $\mathscr{L}_A(M_\lambda)$ и, следовательно, над кольцом C, так как $cx = c_\lambda(x)$ при любых $x \in M_\lambda$, $c \in C$. Поскольку подмодуль M_λ устойчив относительно бикоммутанта A-модуля M (§ 1, n° 4, предложение 21) (§ 1, n° 3, предложение 5), то модуль M_λ равен сумме изотипных компонент C-модуля M (§ 3, n° 4, предложение 11); следовательно, M_λ является изотипной компонентой C-модуля M.

5. *Применения: Устойчивые подмодули тензорных произведений*

Предложение 6. *Пусть* S *— простой* A*-модуль,* D *— его коммутант,* T *— правое векторное пространство над* D, $\mathscr{F}$ *— множество эндоморфизмов пространства* T. *Для того чтобы подмодуль* A*-модуля* $T \otimes_D S$ *был устойчив относительно всех эндоморфизмов*

$u \otimes 1$, где u пробегает $\mathscr{F}$, необходимо и достаточно, чтобы он имел вид $T' \otimes_D S$, где T' — векторное подпространство в T, устойчивое относительно всех эндоморфизмов $u \in \mathscr{F}$.

В самом деле, $(u \otimes 1)(T' \otimes_D S) = u(T') \otimes_D S$; предложение следует из того, что отображение $T' \to T' \otimes_D S$ является изоморфизмом (для структуры порядка по включению) множества векторных подпространств пространства T на множество подмодулей произведения $T \otimes_D S$ (n° 4, следствие предложения 4).

Предложение 7. *Пусть E — тело, M — множество эндоморфизмов E на его подтела, D — подтело, состоящее из элементов E, инвариантных относительно всех эндоморфизмов $f \in M$. Пусть T — правое векторное пространство над D; наделим $T \otimes_D E$ структурой правого векторного пространства над E. Для того чтобы некоторое подпространство пространства $T \otimes_D E$ было устойчиво относительно всех отображений $1 \otimes f$, где f пробегает множество M, необходимо и достаточно, чтобы оно имело вид $T' \otimes_D E$, где T' — векторное подпространство в T.*

Ясно, что это условие достаточно. Для доказательства необходимости в кольце эндоморфизмов абелевой группы рассмотрим подкольцо, порожденное объединением множества M и кольца B правых умножений пространства E; так как E — простой B-модуль, то E — простой A-модуль. Кроме того, коммутант A-модуля E содержится в коммутанте C B-модуля E, причем C совпадает с кольцом левых умножений пространства E (§ 1, n° 2, предложение 4). Но для того, чтобы левое умножение $x \to ax$ было перестановочно со всеми элементами $f \in M$, необходимо и достаточно, чтобы $a \in D$; иными словами, коммутант A-модуля E отождествляется с D. Теперь предложение вытекает из следствия к предложению 4 n° 4.

Заметим, что предложение 7, по существу, совпадает с предложением 10, гл. II, § 5, n° 5, и таким образом, мы получили новое доказательство этого предложения.

Упражнения. 1) Пусть A — кольцо, $\mathfrak{m}$ — его максимальный левый идеал, B — множество элементов $b \in A$ таких, что $\mathfrak{m}b \subset \mathfrak{m}$. Показать, что B является в A наибольшим подкольцом, содержащим $\mathfrak{m}$ в качестве двустороннего идеала. Пусть M — A-модуль $A_s/\mathfrak{m}$, φ —

каноническое отображение модуля A_s на $A_s/\mathfrak{m}$, D — коммутант модуля M; показать, что формула $u_b(x) = \varphi(ab)$, где $b \in B$, $x = \varphi(a) \in M$, определяет элемент $u_b \in B$; кроме того, отображение $b \to u_b$ является гомоморфизмом кольца B на тело D, и его ядро есть $\mathfrak{m}$.

2) Пусть K — поле, B — алгебра (без единицы) над полем K, имеющая базис e_1, e_2 такой, что $e_1^2 = e_1$, $e_1e_2 = e_2^2 = 0$, $e_2e_1 = e_2$. Пусть M — B-модуль B_s, Ω — кольцо эндоморфизмов абелевой группы M, A — подкольцо Ω, порожденное единичным элементом и кольцом гомотетий B-модуля M. Показать, что:

а) A-модуль M не простой, но в нем имеется простой A-подмодуль N такой, что фактормодуль M/N прост.

б) Коммутант A-модуля M изоморфен полю K.

в) Кольцо гомотетий A-модуля M не плотно в своем бикоммутанте.

3) Пусть M — множество Q рациональных чисел, рассматриваемое как $\mathbf{Z}$-модуль. Каков его бикоммутант? Показать, что M — простой модуль над своим бикоммутантом и что кольцо гомотетий $\mathbf{Z}$-модуля M не плотно в своем бикоммутанте.

4) Пусть K — поле, V — векторное пространство K^4 над K, E_{ij} — элементы канонического базиса алгебры матриц порядка 4 над полем K, отождествленной с кольцом $A = \mathscr{L}_A(V)$ (гл. II, § 7, n° 6). Пусть B — коммутативная подалгебра в A, порожденная единицей и матрицами E_{41}, E_{42} и E_{31}. Показать, что кольцо гомотетий B-модуля V не плотно в своем бикоммутанте.

*5) Пусть A — кольцо главных идеалов, M — A-модуль кручения. Показать, что кольцо гомотетий модуля M плотно в своем бикоммутанте. (Доказать, что всякое подмножество в M содержится в некотором подмодуле N модуля M, обладающем в M дополнением и являющемся прямой суммой конечного числа неразложимых делимых модулей и модуля конечного типа; для этого воспользоваться предложением 5 § 1, n° 3, и упражнениями 3 и 8 гл. VII, § 2; применить затем теорему 2 гл. VII, § 4, n° 3.)

*6) Пусть V — векторное пространство над телом D размерности $\geqslant 2$, $A = \mathscr{L}_D(V)$ — кольцо эндоморфизмов пространства V, B — подкольцо в A, содержащее единицу кольца A.

а) Предположим, что для любой системы из четырех элементов x_1, x_2, y_1, y_2 пространства V, в которой элементы x_1, x_2 линейно независимы, существует $u \in B$ такой, что $u(x_1) = y_1$, $u(x_2) = y_2$. Показать, что тело D (отождествленное с кольцом гомотетий пространства V) является коммутантом B в кольце Ω эндоморфизмов абелевой группы V и B плотно в Ω относительно своего бикоммутанта.

б) Привести пример подкольца B в кольце A, содержащего единицу кольца A, такого, что B-модуль V прост, но коммутант B в Ω отличен от D (рассмотреть случай, когда пространство V получается из некоторого векторного пространства над некоторым надтелом D'

тела D сужением на D тела скаляров, и в качестве B взять кольцо D_0-эндоморфизмов).

7) Пусть S — простой A-модуль, D — его коммутант, M — изотипный полупростой A-модуль типа S, C — его коммутант, C' — его бикоммутант.

а) Показать, что кольцо $C \cap C'$ изоморфно центру тела D.

б) Пусть L — подкольцо в кольце Ω эндоморфизмов абелевой группы M, порожденное объединением кольца C и кольца A_M гомотетий модуля M. Показать, что M — простой L-модуль.

*8) A-модуль M называется *соизмеримым* с A_s, если существуют целые числа $m > 0$, $n > 0$ такие, что модуль A_s^m изоморфен M^n.

а) Пусть M — модуль конечной длины, соизмеримый с A_s. Показать, что кольцо A артиново и нетерово, если m' и n' — еще два числа такие, что $A_s^{m'}$ изоморфен $M^{n'}$, то $m/n = m'/n'$ (использовать теорему 1 § 2, n° 2); m/n называют *рангом* модуля M над A.

б) Пусть C — коммутант модуля M, M' — контрмодуль модуля M; показать, что если модуль A_s^m изоморфен M^n, то модуль $C_s^{n^2}$ изоморфен M'^{mn} (положив $N = M^n$ и применяя теорему 1 и упражнение 8в) § 1, рассмотреть $\mathscr{L}_A(N)$ как C-модуль).

в) Вывести из а) и б), что если модуль M конечной длины соизмерим с A_s и ранг его над A равен r, то модуль M' конечной длины соизмерим с C_s и имеет над C ранг $1/r$ (использовать упражнение 5д) § 2).

г) Пусть B — кольцо главных идеалов, $\mathfrak{a}$ — его двусторонний идеал и $A = B/\mathfrak{a}$. Показать, что ранг всякого A-модуля M, соизмеримого с A, есть целое число и равен рангу, определенному в упражнении 8 гл. VII, § 4.

9) Пусть V — бесконечномерное векторное пространство над телом D, A — плотное подкольцо в $\mathscr{L}_D(V)$. Показать, что для всякого целого числа $n > 0$ найдется подкольцо B кольца A, содержащее его единицу и отображающееся гомоморфно на матричную алгебру $M_n(D^0)$.

10) а) Пусть E — простой A-модуль, у которого сопряженный модуль E^* — тоже простой A-модуль, и E^{**} отождествляется с E; показать, что тело, коммутант модуля E, изоморфно телу, противоположному коммутанту модуля E^*.

б) *Кодлиной* простого A-модуля M называется размерность контрмодуля модуля M (над коммутантом модуля M). A-модуль конечной длины N называют модулем *конечной кодлины*, если в некотором ряде Жордана — Гельдера $N_0 = N \supset N_1 \supset \ldots \supset N_r = \{0\}$ кодлины простых модулей N_i/N_{i+1} $(1 \leqslant i \leqslant r-1)$ конечны; сумма этих кодлин называется *кодлиной* модуля N. Пусть $\lambda(N)$ — кодлина A-модуля N конечной кодлины и P — подмодуль N. Тогда $\lambda(N) = \lambda P + \lambda(N/P)$.

Пусть A — *инволютивное* кольцо (§ 2, упражнение 11), и модули A_s и A_d — конечной кодлины. Кольцо A называется *фробениусовым*.

если $\lambda(M) = \lambda(M^*)$ для любого простого A-модуля M; показать, что в этом случае $\lambda(E) = \lambda(E^*)$ для любого A-модуля E конечной длины. Пусть A — фробениусова алгебра конечного ранга над полем K; вывести из а), что $\dim_K(E) = \dim_K(E^*)$ для любого A-модуля E конечной длины.

в) Пусть K — поле, A — подалгебра матричной алгебры $M_6(K)$ с базисом $E_{11}+E_{55}$, $E_{12}+E_{56}$, $E_{21}+E_{65}$, $E_{22}+E_{66}$, $E_{33}+E_{44}$, E_{13}, E_{23}, E_{45} и E_{46} (E_{ij} — элемеиты канонического базиса алгебры $M_6(K)$). Показать, что алгебра A инволютивна, но не фробениусова. (Заметить, что минимальные левые идеалы в алгебре A — это $KE_{13}+KE_{23}$, KE_{45} и KE_{46}, минимальные правые идеалы KE_{13}, KE_{23}, $KE_{45}+KE_{46}$.)

§ 5. Простые и полупростые кольца

1. *Полупростые кольца*

Предложение 1. *Пусть A — кольцо; следующие свойства эквивалентны:*

а) *всякий A-модуль полупрост;*

б) *модуль A_s полупрост.*

В самом деле, всякий A-модуль изоморфен фактормодулю модуля $A_s^{(I)}$ (гл. II, § 1, n° 8, предложение 10), а фактормодуль полупростого модуля полупрост (§ 3, n° 3, следствие предложения 8). Поэтому из б) следует а).

Определение 1. *Кольцо A называется полупростым, если оно обладает эквивалентными свойствами* а) *и* б) *из предложения* 1.

Замечание. Пусть A — полупростое кольцо; модуль A_s моногенен (порождается единицей) и имеет конечную длину (§ 3, n° 5, предложение 13); следовательно, кольцо A артиново и нетерово.

Предложение 2. *Кольцо A^0, противоположное полупростому кольцу A, полупросто.*

В самом деле, A^0-модуль $(A^0)_s$ есть A^0-модуль A_r, то есть контрмодуль модуля A_s (§ 1, n° 2, предложение 4). Однако контрмодуль полупростого модуля полупрост (§ 4, n° 4, предложение 5).

Предложение 3. *Пусть M — A-модуль, и его контрмодуль является модулем конечного типа. Для того чтобы кольцо гомотетий A_M было полупросто, необходимо и достаточно, чтобы модуль M был полупрост.*

Необходимость этого условия очевидна. Обратно, если модуль M полупрост, то модуль $(A_M)_s$, изоморфный некоторому подмодулю произведения M^n ($n > 0$ — целое число), полупрост по лемме 4 § 2, n° 3.

Предложение 4. *Для того чтобы кольцо было полупростым, необходимо и достаточно, чтобы оно было изоморфно кольцу эндоморфизмов некоторого полупростого модуля конечной длины.*

Контрмодуль полупростого модуля полупрост (§ 4, n° 4, предложение 5), и достаточность условия следует из предложения 3. Обратно, пусть кольцо A полупросто. Тогда модуль A полупрост и моногенен (предложение 2), а кольцо A изоморфно кольцу его эндоморфизмов (§ 1, n° 2, предложение 4).

Предложение 5. *Пусть A — полупростое кольцо. Отличные от $\{0\}$ изотипные компоненты A-модуля A_s являются минимальными двусторонними идеалами кольца A. Всякий двусторонний идеал кольца A является прямой суммой минимальных двусторонних идеалов.*

В самом деле, двусторонние идеалы кольца A являются подмодулями в A_s, устойчивыми относительно правых умножений кольца A, то есть относительно коммутанта модуля A_s (§ 1, n° 2, предложение 4). Следовательно (§ 3, n° 4, предложение 11), они являются прямыми суммами изотипных компонент модуля A_s, а минимальные двусторонние идеалы — изотипными компонентами модуля A_s, что и доказывает предложение.

Предложение 6. *Пусть A — полупростое кольцо. Всякий простой A-модуль изоморфен некоторому минимальному левому идеалу кольца A.*

В самом деле, всякий простой A-модуль изоморфен фактормодулю модуля A_s и, значит, некоторому простому подмодулю модуля A_s, ибо A_s полупрост (§ 3, n° 3, предложение 8).

Предложение 7. *Пусть A — полупростое кольцо, для любого его левого идеала $\mathfrak{l}$ существует такой идемпотент $e \in \mathfrak{l}$, что $\mathfrak{l} = Ae = \mathfrak{l}e$.*

В самом деле, идеал $\mathfrak{l}$ обладает в A_s дополнением $\mathfrak{l}'$ (§ 3, n° 3, предложение 7). Пусть $1 = e + e'$, $e \in \mathfrak{l}$, $e' \in \mathfrak{l}'$; для любого $x \in \mathfrak{l}$ имеем $x = xe + xe'$; но $xe \in \mathfrak{l}$, $xe' \in \mathfrak{l}'$, и поэтому $xe = x$, $xe' = 0$. Это доказывает, что $e^2 = e$ и $\mathfrak{l} = \mathfrak{l}e$. Так как $Ae \subset \mathfrak{l} = \mathfrak{l}e \subset Ae$, то $\mathfrak{l} = Ae$.

2. *Простые кольца*

Предложение 8. *Пусть A — полупростое кольцо. Следующие свойства эквивалентны:*

а) *существует только один класс простых A-модулей;*

б) *полупростой A-модуль A_s изотипен;*

в) *A и $\{0\}$ — единственные двусторонние идеалы кольца A.*

Эквивалентность свойств б) и в) следует из предложения 5. Ясно, что, с другой стороны, б) следует из а). Наконец, а) следует из б): модуль A_s изотипен, так что всякий A-модуль, будучи изоморфен фактормодулю модуля $A_s^{(I)}$ (гл. II, § 1 n° 8, предложение 10), изотипен (§ 3, n° 3, предложение 8).

Определение 2. *Полупростое кольцо называется простым, если оно не сводится к 0 и обладает свойствами* а), б) *и* в) *предложения* 8.

Ниже мы увидим (§ 6, n° 4), следствие 4 теоремы 4), что простые кольца можно охарактеризовать как артиновы кольца, не сводящиеся к 0, единственными двусторонними идеалами которых являются A и $\{0\}$.

Примеры. 1) Всякое тело D — простое кольцо, так как D_s — простой D-модуль.

2) Всякое *коммутативное* простое кольцо — поле (гл. I, § 9, n° 3, предложение 3).

Алгебра A называется *простой* (соответственно *полупростой*), если A проста (соответственно полупроста) как кольцо.

Предложение 9. *Пусть M — A-модуль, и его контрмодуль конечного типа. Для того чтобы кольцо гомотетий A_M было просто, необходимо и достаточно, чтобы M был изотипным полупростым модулем.*

Необходимость условия очевидна. Обратно, если M — изотипный полупростой модуль, то модуль $(A_M)_s$, изоморфный подмодулю произведения M^n ($n > 0$ — целое число) (§ 2, n° 3, лемма 4),— изотипный полупростой (§ 3, n° 3, предложение 8).

3. *Простые компоненты полупростого кольца*

Теорема 1. *Полупростое кольцо A имеет конечное число минимальных двусторонних идеалов A_i $(1 \leqslant i \leqslant n)$. Каждый идеал A_i является простым кольцом с единицей, и кольцо A является прямой композицией подколец A_i. Обратно, пусть $(A_i)_{1 \leqslant i \leqslant n}$ — конечное семейство простых колец. Произведение A колец A_i полупросто, и канонические образы колец A_i в A являются в A минимальными двусторонними идеалами.*

Пусть A — полупростое кольцо. Модуль A_s обладает лишь конечным числом изотипных компонент (n° 1, замечание), то есть (n° 1, предложение 5) минимальных двусторонних идеалов A_i $(1 \leqslant i \leqslant n)$. Кольцо A является прямой суммой и, следовательно (гл. I, § 8, n° 11, предложение 7), прямой композицией идеалов A_i; компонента единицы кольца A в каждом A_i будет единицей кольца A_i. Идеалы A_i взаимно аннулируются, так что каждый модуль $(A_i)_s$ имеет то же самое кольцо гомотетий, что и подмодуль A_i модуля A_s, то есть кольца A_i полупросты; кроме того, всякий двусторонний идеал кольца A_i является двусторонним идеалом в кольце A, откуда следует, что кольцо A_i просто.

Обратно, пусть $(A_i)_{1 \leqslant i \leqslant n}$ — конечное семейство простых колец, и A — их произведение. Очевидно, A_i являются двусторонними минимальными идеалами в A (гл. I, § 8, n° 10, предложение 6). С другой стороны, A_i являются простыми подмодулями в A-модуле A_s; следовательно, модуль A_s полупрост, и A — полупростое кольцо.

Определение 3. *Минимальные двусторонние идеалы полупростого кольца называются его простыми компонентами.*

Предложение 10. *Всякое факторкольцо полупростого кольца A полупросто и изоморфно некоторому подкольцу в A, то есть сумме простых компонент кольца A.*

Это следует из предложения 5 n° 1 и теоремы 1.

Если $\mathfrak{a}$ — двусторонний идеал кольца A, то всякий $(A/\mathfrak{a})$-модуль отождествляется с некоторым A-модулем и, следовательно, полупрост; это непосредственно доказывает первую часть предложения 10.

Предложение 11. *Пусть A — полупростое кольцо, $(A_i)_{1\leqslant i\leqslant r}$ — семейство его простых компонент. Существует r классов простых A-модулей. Для любого простого A-модуля S существует единственный индекс i $(1\leqslant i\leqslant r)$ такой, что $A_iS\neq\{0\}$; модуль S, рассматриваемый над кольцом A_i, прост.*

Ввиду предложения 6 n° 1 достаточно заметить, что всякий минимальный левый идеал кольца A является минимальным левым идеалом в одной и только в одной компоненте A_i (гл. I, § 8, n° 10, предложение 6).

Простые A-модули, соответствующие компонентам A_i и A_j, $i\neq j$, не изоморфны, даже если A_i и A_j изоморфны *как кольца*: в самом деле, они имеют различные аннуляторы.

4. Строение простых колец

Теорема 2. а) *Пусть M — векторное пространство конечной размерности r над телом D. Кольцо $A=\mathscr{L}_D(M)$ эндоморфизмов модуля M (изоморфное кольцу матриц $\mathbf{M}_r(D^0)$ над противоположным телом D^0* (гл. II, § 6, n° 5)) *просто. Изотипный модуль A_s имеет длину r. A-модуль M прост.*

б) *Обратно, пусть A — простое кольцо, модуль A_s имеет длину r, M — простой A-модуль, D — тело, коммутант модуля M. Тогда $\dim_D(M)=r$ и гомоморфизм $a\to a_M$ кольца A в $\mathscr{L}_D(M)$ биективен.*

Пусть M — векторное пространство конечной размерности r над телом D и $A=\mathscr{L}_D(M)$. A-модуль M точный и простой (§ 3, n° 1, пример 2). С другой стороны, пусть $(x_1, x_2, \ldots, x_r)$ — базис M над телом D. Отображение $a\to(ax_1, ax_2, \ldots, ax_r)$ является инъективным A-гомоморфизмом модуля A_s в M^r (§ 2, n° 3, лемма 4); ясно также, что этот гомоморфизм сюръективен (гл. II, § 2, n° 4, следствие 2 предложения 3). Следовательно, модуль A_s — изотипный модуль длины r, и кольцо A просто (n° 2, предложение 8).

Обратно, пусть A — простое кольцо и M — простой A-модуль. Коммутант D модуля M — тело (§ 4, n° 3, предложение 2). Кольцо гомотетий модуля A_s совпадает с его бикоммутантом (§ 1, n° 2, следствие предложения 4); бикоммутант модуля B, то есть $\mathscr{L}_D(M)$, отождествляется с бикоммутантом модуля A_s, то есть с кольцом A:

это следует из предложения 8 § 1, n° 3, и того, что модуль A_s — изотипный типа M (n° 2, предложение 8). Наконец, размерность $\dim_D(M)$ конечна, так как в противном случае кольцо $\mathscr{L}_D(M)$ было бы не артиновым (§ 2, n° 3, пример 4), что неверно (n° 1, пример 1); из первой части доказательства следует равенство $\dim_D(M) = l_A(A_s)$.

Замечание. Пусть A — простое кольцо. Так как все простые A-модули A-изоморфны, то тело D в теореме 2б) однозначно, с точностью до изоморфизма, определяется заданием лишь кольца A. Отсюда получается следствие: пусть M_1 (соответственно M_2)— конечномерное векторное пространство над телом D_1 (соответственно D_2); если кольца $\mathscr{L}_{D_1}(M_1)$ и $\mathscr{L}_{D_2}(M_2)$ изоморфны, то тела D_1 и D_2 изоморфны и $\dim_{D_1}(M_1) = \dim_{D_2}(M_2)$.

Следствие 1. *Пусть A — кольцо, M — изотипный полупростой A-модуль конечной длины r, $B = \mathscr{L}_A(M)$. Кольцо B просто, и $l_B(B_s) = r$.*

По предложению 4 § 4, n° 4, кольцо B изоморфно кольцу эндоморфизмов некоторого векторного пространства размерности r, и достаточно, следовательно, применить теорему 2.

Следствие 2. *Пусть M — модуль над полупростым кольцом A. Контрмодуль модуля M конечного типа, бикоммутант модуля M совпадает с кольцом гомотетий.*

Второе утверждение следует из первого (§ 4, n° 2, следствие 1 теоремы 1). Так как модуль M обладает лишь конечным числом изотипных компонент (n° 3, предложение 11), то доказательство сводится к случаю, когда модуль M изотипен. Тогда длина его контрмодуля равна размерности простого A-модуля S над его коммутантом D (§ 4, n° 4, предложение 4в)). Однако модуль S можно рассматривать как простой модуль над одной из простых компонент кольца A (n° 3, предложение 11). Тогда по теореме 2 размерность $\dim_D(S)$ конечна.

Следствие 3. *Если кольцо A просто, то и его противоположное кольцо A^0 просто, и $l_A(A_s) = l_{A^0}(A_s^0) = l_{A^0}(A_r)$.*

В самом деле, отображение $U \to {}^tU$ является изоморфизмом кольца матриц $\boldsymbol{M}_r(D^0)$ на кольцо, противоположное кольцу матриц $\boldsymbol{M}_r(D)$ (гл. II, § 6, n° 6).

Предложение 12. а) *Центр простого кольца A — поле. Более точно, если A — кольцо $\mathfrak{L}_D(M)$ эндоморфизмов векторного пространства M над телом D, то центр A есть кольцо центральных гомотетий M, изоморфное центру тела D.*

б) *Центр полупростого кольца является прямой композицией центров его простых компонент.*

Утверждение а) следует из описания центра кольца эндоморфизмов свободного модуля (гл. II, § 2, n° 5, следствие 1 предложения 5). Утверждение б) немедленно вытекает из определения произведения колец (см. гл. I, § 8, n° 11).

Следствие 1. *Полупростое кольцо просто тогда и только тогда, когда его центр — поле.*

Если A — простая алгебра над полем K, то ее центр Z является расширением поля K; если $Z = K$, то алгебра A называется центральной.

Следствие 2. *Всякая простая центральная алгебра A конечного ранга над полем K K-изоморфна алгебре матриц $\mathbf{M}_r(L)$, где L — тело с центром K конечного ранга над K.*

В самом деле, если $\mathfrak{L}_D(M)$ (обозначения из предложения 12) имеет конечный ранг над центром K тела D, то тело D имеет конечный ранг над K (гл. III, § 3, n° 2).

Следствие 3. *Всякая простая алгебра конечного ранга над* алгебраически замкнутым *полем K центральна и изоморфна некоторой алгебре матриц $\mathbf{M}_r(K)$.*

Это вытекает из следствия 2 и леммы 3 § 4, n° 3.

5. *Полупростые подалгебры полупростых алгебр*

Теорема 3. *Пусть K* — алгебраически замкнутое *поле, A — полупростая алгебра конечного ранга над полем K, B — полупростая подалгебра в A, содержащая ее единицу. Пусть S — простой A-модуль, T — простой B-модуль. Тогда S, рассматриваемый как B-модуль, имеет изотипную компоненту типа T; длина этой компоненты конечна и равна длине изотипной компоненты типа S тензорного произведения $A \otimes_B T$, рассматриваемого как A-модуль, а также длине изотипной компоненты типа S*

в $\mathscr{L}_B(A, T)$, *рассматриваемом как A-модуль* (см. гл. III, приложение II, n° 7)*).

Все рассматриваемые модули конечномерны над K (n° 4, теорема 2б)) и унитарны, так как, по предположению, A и B имеют одну и ту же единицу. Так как поле K алгебраически замкнуто, то тело гомотетий K_S (соответственно K_T) совпадает с коммутантом модуля S (соответственно T) (§ 4, n° 3, следствие 1 предложения 2). Из предложения 3 § 4, n° 3, и его следствия вытекает поэтому, что длина изотипной компоненты типа T в S (рассматриваемом как B-модуль) равна $\dim_K \mathscr{L}_B(T, S) = \dim_K \mathscr{L}_B(S, T)$. Из тех же соображений длина изотипной компоненты типа S в $A \otimes_B T$ (рассматриваемом как A-модуль) равна $\dim_K \mathscr{L}_A(A \otimes_B T, S)$, а длина изотипной компоненты типа S в $\mathscr{L}_B(A, T)$ (рассматриваемом как A-модуль) равна $\dim_K \mathscr{L}_A(S, \mathscr{L}_B(A, T))$. Наконец, в предложении 7 гл. III, приложение II, n° 8, установлены канонические изоморфизмы абелевых групп

$$\mathscr{L}_A(A \otimes_B T, S) \to \mathscr{L}_B(T, \mathscr{L}_A(A, S)) = \mathscr{L}_B(T, S)$$

и

$$\mathscr{L}_A(S, \mathscr{L}_B(A, T)) \to \mathscr{L}_B(A \otimes_A S, T) = \mathscr{L}_B(S, T);$$

из определения этих изоморфизмов немедленно следует, что они будут также изоморфизмами для структур рассматриваемых векторных K-пространств; отсюда и следует теорема.

Следствие. *Пусть* A, B, K *те же, что в теореме* 3, $\mathfrak{l}_A$ — *минимальный левый идеал в* A, $\mathfrak{l}_B$ — *минимальный левый идеал в* B, $\mathfrak{n}_A$ — *левый идеал в* A, *порожденный* $\mathfrak{l}_B$. *Тогда*

$$[\mathfrak{n}_A : \mathfrak{l}_A] = [\mathfrak{l}_A : \mathfrak{l}_B], \tag{1}$$

где в правой части $\mathfrak{l}_A$ *рассматривается как B-модуль.*

Идеал $\mathfrak{n}_A$ состоит из сумм $\sum_i a_i x_i$, где $a_i \in A$, $x_i \in \mathfrak{l}_B$. Но $\boldsymbol{Z}$-билинейное отображение $(a, x) \to ax$ произведения $A \times \mathfrak{l}_B$ в A обладает свойством $(ab)\,x = a\,(bx)$ для любого $b \in B$; поэтому ему соответствует (гл. III, приложение I, n° 1, предложение 2) $\boldsymbol{Z}$-линейное отображение φ тензорного произведения $A \otimes_B \mathfrak{l}_B$ в A; это отображение φ также и A-линейно; идеал $\mathfrak{n}_A$ является обра-

*) Напомним (там же), что для этой структуры произведение αu элемента $\alpha \in A$ и B-гомоморфизма u алгебры A в T есть B-гомоморфизм $\xi \to u(\xi\alpha)$.

зом при отображении φ A-модуля $A \otimes_B \mathfrak{l}_B$. Ввиду теоремы 3 остается лишь доказать, что φ инъективно. Пусть $e \in \mathfrak{l}_B$ — такой идемпотент, что $\mathfrak{l}_B = Be$ (n° 1, предложение 7); всякий элемент модуля $A \otimes_B \mathfrak{l}_B$ может быть записан в виде $a \otimes e$, $a \in A$, и соотношение $0 = \varphi(a \otimes e) = ae$ влечет $0 = (ae) \otimes e = a \otimes (e^2) = a \otimes e$, откуда и следует доказываемое утверждение.

6. *Степени, высоты, индексы*

Предложение 13. *Пусть B — простое кольцо, r — длина модуля B_s, M — B-модуль.*

а) *Модуль M свободен тогда и только тогда, когда длина $l_B(M)$ бесконечна или кратна r.*

б) *В этом случае для любого базиса $(u_\iota)_{\iota \in I}$ модуля M выполняется равенство $l_B(M) = r \operatorname{Card}(I)$ (откуда следует, что $\operatorname{Card}(I)$ не зависит от выбора этого базиса).*

в) *Если на модуле M существует структура правого B-модуля такая, что $(bx)\,b' = b\,(xb')$ для $b \in B$, $b' \in B'$, $x \in M$, то M — свободный левый B-модуль.*

В самом деле, пусть M — свободный модуль с базисом $(u_\iota)_{\iota \in I}$. Тогда M есть прямая сумма подмодулей Bu_ι, каждый из которых B-изоморфен B_s и имеет, следовательно, длину r; поэтому $l_B(M) = r \operatorname{Card}(I)$. Ясно, что, обратно, если длина $l_B(M)$ бесконечна или конечна и кратна r, то M — прямая сумма подмодулей, изоморфных B_s, и, следовательно, свободна. Это доказывает утверждения а) и б). Пусть теперь выполнено условие в). Левый B-модуль изоморфен левому B-модулю $M \otimes_B B_s$ (гл. III, приложение II, n°n° 3 и 4); так как модуль B_s является прямой суммой r B-изоморфных левых модулей, то и $M \otimes_B B_s$ является прямой суммой r B-изоморфных левых модулей, откуда следует, что $l_B(M)$ бесконечна или кратна r.

Следствие. *Пусть A — кольцо, B — простое подкольцо в A, содержащее его единицу. Кольцо A, рассматриваемое как левый модуль над кольцом B, является свободным модулем, и все базисы этого B-модуля равномощны.*

В самом деле, структуры левого и правого A-модулей, определенные на кольце A его умножением, унитарны и удовлетворяют условию в) предложения 13.

Предположение, что подкольцо B содержит единицу кольца A, обеспечивает унитарность структур B-модуля на кольце A; без этого предположения следствие неверно: это видно из примера, в котором A является прямой композицией подкольца B и произвольного второго подкольца.

Определение 4. *Пусть A — кольцо, и B — простое подкольцо в A, содержащее его единицу. Степенью кольца A над B называется кардинальное число любого базиса кольца A, рассматриваемого как левый B-модуль. Степень кольца A над B обозначается* $[A : B]$.

Если B — тело, то $[A : B]$ совпадает с размерностью A, рассматриваемого как левое векторное пространство над B.

Кольцо B^0 просто (n° 4, следствие 3 теоремы 2), и можно определить степень $[A^0 : B^0]$ как кардинальное число любого базиса A, рассматриваемого как правый B-модуль. Однако числа $[A : B]$ и $[A^0 : B^0]$ не обязаны быть равными даже в случае, когда B — тело; одно из них может быть конечно, а другое бесконечно (§ 2, упражнение 4).

Предложение 14. *Пусть A — кольцо, B — простое подкольцо в A, C — простое подкольцо в B, B и C содержат единицу кольца A. Тогда* $[A : C] = [A : B]\,[B : C]$.

В самом деле, пусть $(a_\alpha)_{\alpha\in I}$ — базис кольца A, рассматриваемого как левый B-модуль, и $(b_\beta)_{\beta\in J}$ — базис кольца B, рассматриваемого как левый C-модуль. Тогда семейство $(b_\beta a_\alpha)_{(\alpha,\,\beta)\in I\times J}$ является базисом A, рассматриваемого как левый C-модуль.

Предложение 15. *Пусть A — кольцо, B — простое подкольцо в A, содержащее его единицу, M — левый B-модуль. Тогда $l_B(A \otimes_B M) = [A : B]\, l_B(M)$, где $A \otimes_B M$ рассматривается как левый B-модуль.*

Пусть S — простой B-модуль, и m — длина левого B-модуля $A \otimes_B S$; имеем равенство $l_B(A \otimes_A M) = m l_B(M)$. Следовательно, предложение 15 достаточно доказать для *одного* B-модуля M конечной длины, не сводящегося к 0. Однако при $M = B_s$ произведение $A \otimes_B M$ изоморфно левому B-модулю A (гл. III, приложение II, n°n° 3 и 4) и длина $l_B(A \otimes_B M)$ равна $[A : B]\, l_B(B_s)$ (предложение 13б)), что и заканчивает доказательство.

Определение 5. *Пусть A — простое кольцо, и B — простое подкольцо в A, содержащее его единицу. Индексом подкольца B в A называется длина A-модуля $A \otimes_B N$, где N — простой левый B-модуль. Этот индекс обозначается $i(A, B)$. Высотой кольца A над подкольцом B называется длина B-модуля, получаемого из некоторого простого A-модуля сужением кольца операторов до B. Высота A над B обозначается $h(A, B)$.*

Если A и B — алгебры конечного ранга над алгебраически замкнутым полем, то по теореме 3 $i(A, B) = h(A, B)$.

Так как модуль A_s изоморфен левому A-модулю $A \otimes_B B_s$ (гл. III, приложение II, n° 4) и B_s является прямой суммой $l_B(B_s)$ подмодулей, изоморфных N, то имеем равенство

$$l_A(A_s) = i(A, B)\, l_B(B_s). \tag{2}$$

С другой стороны, пусть P — левый A-модуль; по определению $h(A, B)$ формула

$$l_B(P) = h(A, B)\, l_A(P) \tag{3}$$

справедлива для простого A-модуля P, а следовательно, и для любого модуля P. Наконец, применяя формулу (3) и предложение 15, получаем равенство $[A : B] = l_B(A \otimes_B N) = h(A, B)\, l_A(A \otimes_B N)$, то есть

$$[A : B] = h(A, B)\, i(A, B). \tag{4}$$

Из формулы (2) следует, что индекс $i(A, B)$ всегда конечен, а формула (4) показывает, что *степень* $[A : B]$ *конечна тогда и только тогда, когда конечна высота* $h(A, B)$.

Пусть C — простое подкольцо в B, содержащее его единицу. Из формул (2) и (3) следуют равенства

$$i(A, C) = i(A, B)\, i(B, C), \tag{5}$$

$$h(A, C) = h(A, B)\, h(B, C). \tag{6}$$

Предложение 16. *Пусть A — простое кольцо, B — простое подкольцо в A, содержащее его единицу, M — A-модуль $\neq \{0\}$. Если длина $l_B(M)$ конечна, то*

а) *коммутант B' B-модуля M — простое кольцо, и коммутант A' A-модуля M является в B' простым подкольцом, содержащим единицу B';*

б) $i(B', A') = h(A, B)$, $h(B', A') = i(A, B)$, $[B' : A'] = [A : B]$.

По формуле (3) $l_B(M) = h(A, B)\, l_A(M)$, то есть $h(A, B)$ и $l_A(M)$ конечны. Отсюда по следствию 1 теоремы 2, n° 4, кольца A' и B' просты и $l_{A'}(A'_s) = l_A(M)$, $l_{B'}(B'_s) = l_B(M) = h(A, B)\, l_A(M)$. Ввиду формулы (2) получаем $i(B', A') = h(A, B)$. A'-модуль M имеет конечную длину, и кольца гомотетий A_M и B_M совпадают со своими бикоммутантами (n° 4, следствие 2 теоремы 2); поэтому можно поменять ролями, с одной стороны, A и B' и, с другой стороны, B и A'; отсюда $h(B', A') = i(A, B)$. Из формулы (4) следует тогда, что $[B' : A'] = [A : B]$.

Упражнения. 1) Пусть A — полупростое кольцо. Показать, что длины A-модуля A_s и A^0-модуля A_r равны.

2) Пусть A — полупростое кольцо, A_i $(1 \leqslant i \leqslant r)$ — его простые компоненты, S_i — простой A-модуль, изоморфный минимальному идеалу кольца A_i $(1 \leqslant i \leqslant r)$, m_i $(1 \leqslant i \leqslant r)$ — длина A_i-модуля (или A-модуля) $(A_i)_s$. Пусть M — A-модуль, n_i — длина его изотипной компоненты типа S_i $(1 \leqslant i \leqslant r)$; показать, что модуль M моногенен тогда и только тогда, когда $n_i \leqslant m_i$ при всех i, $1 \leqslant i \leqslant r$.

*3) Пусть V — векторное пространство над телом D, $A = \mathscr{L}_D(V)$ — его кольцо эндоморфизмов.

а) Обозначим через $\mathfrak{r}(M)$ (соответственно $\mathfrak{l}(M)$), где M — векторное подпространство в V, правый (соответственно левый) идеал кольца A, состоящий из эндоморфизмов u пространства V таких, что $u(V) \subset M$ (соответственно $u^{-1}(0) \supset M$). Показать, что отображение $M \to \mathfrak{r}(M)$ (соответственно $M \to \mathfrak{l}(M)$) является строго возрастающим (соответственно строго убывающим) отображением множества векторных подпространств пространства V на множество правых (соответственно левых) идеалов кольца A, обладающих дополнением в A_s (соответственно в A_d), или, что то же самое, порожденных идемпотентом кольца A (см. § 1, упражнение 2). Имеют место равенства:

$$\mathfrak{r}(M+N) = \mathfrak{r}(M) + \mathfrak{r}(N), \qquad \mathfrak{r}(M \cap N) = \mathfrak{r}(M) \cap \mathfrak{r}(N),$$
$$\mathfrak{l}(M+N) = \mathfrak{l}(M) \cap \mathfrak{l}(N), \qquad \mathfrak{l}(M \cap N) = \mathfrak{l}(M) + \mathfrak{l}(N).$$

б) Для того чтобы правый идеал $\mathfrak{r}$ (соответственно левый идеал $\mathfrak{l}$) кольца A был минимальным, необходимо и достаточно, чтобы он имел вид $\mathfrak{r}(M)$, где размерность M равна 1 (соответственно вид $\mathfrak{l}(M)$, где факторразмерность M равна 1). Вывести отсюда, что правый идеал $\mathfrak{r}$ (соответственно левый идеал $\mathfrak{l}$) имеет конечную длину m тогда и только тогда, когда он имеет вид $\mathfrak{r}(M)$, где размерность M равна m (соответственно вид $\mathfrak{l}(M)$, где факторразмерность M равна m). Рассмотреть частный случай, когда пространство V конечномерно.

в) Пусть M, N — подпространства в V, $M \neq \{0\}$ и $N \neq V$. Показать, что пересечение $\mathfrak{r}(M) \cap \mathfrak{l}(N)$ не сводится к 0.

г) Пусть V^* — сопряженное к V пространство, рассматриваемое как левое векторное пространство над D^0. Отображение $u \to {}^t u$ является изоморфизмом кольца A на некоторое подкольцо B кольца, противоположного $\mathscr{L}_{D^0}(V)$. Показать, что при этом гомоморфизме образ $\mathfrak{r}(M)$ (соответственно $l(M)$) есть след на B идеала $\mathfrak{l}(M^0)$ (соответственно $\mathfrak{r}(M^0)$), где M^0 — подпространство в V, ортогональное к M.

д) Пусть пространство V имеет бесконечную размерность $\mathfrak{c}$. Пусть $\mathfrak{r}$ — правый идеал в кольце A, $u \in \mathfrak{r}$. Показать, что всякое проектирование пространства V на $u(V)$ принадлежит $\mathfrak{r}$. Пусть $\mathscr{F}(\mathfrak{r})$ — множество подпространств $u(V)$, где u пробегает $\mathfrak{r}$, и $S(\mathfrak{r})$ — сумма этих подпространств. Показать, что: 1° всякое векторное подпространство, содержащееся в некотором $M \in \mathscr{F}(\mathfrak{r})$, принадлежит $\mathscr{F}(\mathfrak{r})$; 2° сумма двух подпространств, принадлежащих $\mathscr{F}(\mathfrak{r})$, принадлежит $\mathscr{F}(\mathfrak{r})$. Доказать обратное утверждение. Показать, что если, в частности, $\mathfrak{m}$ — максимальный правый идеал кольца A, не имеющий вида $\mathfrak{r}(H)$, то $S(\mathfrak{m}) = V$ и $\mathscr{F}(\mathfrak{m})$ — максимальное множество векторных подпространств из V, удовлетворяющее указанным выше условиям 1° и 2°; вывести отсюда, что всякое подпространство $M \in \mathscr{F}(\mathfrak{m})$ имеет бесконечную коразмерность и в $\mathscr{F}(\mathfrak{m})$ имеются подпространства размерности $\mathfrak{c}$. Аналогичные характеристики имеют место для левых идеалов.

*4) Пусть V — векторное пространство бесконечной размерности $\mathfrak{c}$ над телом D; *рангом* эндоморфизма u этого пространства называется размерность (конечная или бесконечная) образа $u(V)$ (равная коразмерности $u^{-1}(0)$); ранг эндоморфизма u обозначается через $\varrho(u)$.

а) Пусть u, v — эндоморфизмы пространства V и $\varrho(u) \leqslant \varrho(v)$. Показать, что существуют элементы a, $b \in A = \mathscr{L}_D(V)$ такие, что $u = avb$.

б) Для любого бесконечного кардинального числа $\mathfrak{n} \leqslant \mathfrak{c}$ через $\mathfrak{A}_\mathfrak{n}$ обозначим множество эндоморфизмов u пространства V, у которых $\varrho(u) < \mathfrak{n}$. Показать, что $\mathfrak{A}_\mathfrak{n}$ является в кольце A двусторонним идеалом и всякий двусторонний идеал кольца A, отличный от $\{0\}$ и от A, равен одному из $\mathfrak{A}_\mathfrak{n}$ (использовать а)). В частности, в кольце A имеется наименьший двусторонний идеал, отличный от $\{0\}$,— идеал $\mathfrak{S}$ эндоморфизмов конечного ранга и наибольший двусторонний идеал $\mathfrak{T} = \mathfrak{A}_\mathfrak{c} \neq A$, состоящий из эндоморфизмов ранга $< \mathfrak{c}$.

°в) Пусть B — базис пространства V, $\mathfrak{U}$ — ультрафильтр на B, более тонкий, чем фильтр $\mathfrak{G}$ дополнений к подмножествам множества B, кардинальные числа которых $< \mathfrak{c}$. Пусть p_U, $U \in \mathfrak{U}$,— проектирование пространства V на подпространство, порожденное элементами подпространства U в разложении V в прямую сумму этого подпространства и подпространства, порожденного элементами $B - U$. Пусть $l_\mathfrak{U}$ — левый идеал кольца A, порожденный идемпотентами $1 - p_U$, где U пробегает $\mathfrak{U}$. Показать, что левый идеал $\mathfrak{T} + \mathfrak{l}_\mathfrak{U}$ отличен от A.

Если $\mathfrak{U}'$ — отличный от $\mathfrak{U}$ ультрафильтр на B, более тонкий, чем $\mathfrak{G}$, то $I_{\mathfrak{U}} + I_{\mathfrak{U}'} = A$.

г) Пусть кардинальное число тела $D \leqslant 2^{\mathfrak{c}}$. Вывести из а), что кардинальное число множества классов простых $(A/\mathfrak{T})$-модулей равно $2^{2^{\mathfrak{c}}}$ (см. § 3, упражнение 2г) и Общ. топол., гл. I, § 8, упражнение 14; в последнем упражнении заметить, что пересечение F и любого элементарного подмножества равномощно с F).

*5) Кольцо A называется *примитивным слева* (или просто *примитивным*), если существует точный простой A-модуль. Кольцо A называется *квазипростым*, если в нем нет двусторонних идеалов, отличных от A и от $\{0\}$.

а) Показать, что всякое квазипростое кольцо примитивно.

б) Показать, что всякое примитивное кольцо изоморфно некоторому плотному подкольцу кольца эндоморфизмов некоторого векторного пространства. Обратно, пусть A — подкольцо кольца эндоморфизмов $\mathscr{L}_D(V)$ векторного пространства V над телом D и для любой пары элементов $x, y \in V$, $x \neq 0$, существует $u \in A$ такой, что $u(x) = y$. Показать, что кольцо A примитивно.

в) Показать, что если кольцо A примитивно, то ненулевые элементы его центра не являются в A делителями нуля (использовать б)). Вывести отсюда, что характеристика кольца A (гл. I, § 8, n° 8) либо 0, либо простое число.

г) Показать, что если кольцо A примитивно (соответственно квазипросто) и $e \in A$ — идемпотент, то кольцо eAe примитивно (соответственно квазипросто) (использовать б), а также упражнение 2в) § 1 и упражнение 5а) § 2)).

д) Пусть A — примитивное кольцо, I и I′ — его левые идеалы. Показать, что если $I \neq \{0\}$ и $I' \neq \{0\}$, то и произведение *) $II' \neq \{0\}$ (использовать б)). Аналогичное свойство справедливо и для правых идеалов. Вывести отсюда, что пересечение конечного числа двусторонних идеалов $\neq\{0\}$ кольца A не равно $\{0\}$.

е) Пусть A — кольцо, для которого существует точный изотипный полупростой A-модуль M. Показать, что A примитивно.

6) Пусть A — примитивное кольцо.

а) Предположим, что элемент $1 + a^2$ при любом $a \in A$ обратим в кольце A. Показать, что A — тело (применить упражнение 5б), показав, что векторное пространство V не может иметь размерность > 1).

б) Предположим, что для любых $a, b \in A$ выполняется равенство $a(ab - ba) = (ab - ba)a$. Показать, что A — тело (тем же методом). В частности, примитивное коммутативное кольцо — поле.

---

*) Определение произведения двух идеалов, используемое в этом и следующих упражнениях, см. в § 6, n° 1.

7) Пусть A — кольцо.

а) Показать, что кольцо матриц $M_r(A)$ примитивно тогда и только тогда, когда примитивно кольцо A (использовать упражнение 5г) и упражнение 9 § 1).

б) Показать, что всякий двусторонний идеал кольца $M_r(A)$ имеет вид $M_r(\mathfrak{a})$, где $\mathfrak{a}$ — двусторонний идеал кольца A. Вывести отсюда, что кольцо $M_r(A)$ квазипросто тогда и только тогда, когда квазипросто кольцо A.

в) Пусть A и B — коммутативные кольца. Показать, что если кольца $M_r(A)$ и $M_r(B)$ изоморфны, то $r = s$ (рассмотреть факторкольца этих колец по максимальным двусторонним идеалам, применяя упражнение б)).

8) а) Пусть A — кольцо, $\mathfrak{r}$ — его минимальный двусторонний идеал. Показать, что либо $\mathfrak{r}^2 = \{0\}$, либо $\mathfrak{r}^2 = \mathfrak{r}$. Во втором случае существует элемент $a \in \mathfrak{r}$ такой, что $a\mathfrak{r} = \mathfrak{r}$; вывести отсюда, что существует идемпотент $e \in \mathfrak{r}$ такой, что $x = ex$ для любого $x \in \mathfrak{r}$, откуда $\mathfrak{r} = eA = e\mathfrak{r}$. Аналогичными свойствами обладают левые минимальные идеалы.

б) Пусть $e \in A$ — идемпотент; eA (соответственно Ae) является минимальным правым (соответственно левым) идеалом тогда и только тогда, когда eAe — тело.

в) Пусть $\mathfrak{r}$, $\mathfrak{r}'$ — изоморфные минимальные правые идеалы кольца A. Показать, что если $\mathfrak{r}^2 = \mathfrak{r}$, то всякий изоморфизм $\mathfrak{r}$ на $\mathfrak{r}'$ имеет вид $x \to a'x$, где $a' \in \mathfrak{r}'$. Показать, что при $\mathfrak{r}'^2 = \mathfrak{r}'$ произведение $\mathfrak{r}\mathfrak{r}'$ равно $\mathfrak{r}$, а при $\mathfrak{r}^k = \{0\}$ равно $\{0\}$.

*9) Пусть A — кольцо. *Правым* (соответственно *левым*) *цоколем* A называется сумма всех его минимальных правых (соответственно левых) идеалов. Правый (соответственно левый) цоколь кольца A является полупростым правым (соответственно левым) A-модулем; изотипные компоненты этого модуля называются *основаниями*.

а) Показать, что всякое основание $\mathfrak{a}$ правого цоколя кольца A является двусторонним идеалом; сумма $\mathfrak{b}$ минимальных правых идеалов с нулевым квадратом, содержащихся в $\mathfrak{a}$, равна пересечению идеала $\mathfrak{a}$ с его правым аннулятором в A и является двусторонним идеалом в A.

б) Пусть некоторое основание $\mathfrak{a}$ правого цоколя кольца A содержит минимальные правые идеалы с квадратом $\neq\{0\}$. Показать, что пересечение $\mathfrak{a}$ с его левым аннулятором в A сводится к 0 (воспользоваться упражнением 5в)).

в) Показать, что в предположениях б) всякий правый идеал кольца $\mathfrak{a}$ (которое, вообще говоря, не имеет единицы) является также правым идеалом в A (заметить, что всякий минимальный правый идеал кольца A, содержащийся в $\mathfrak{a}$, является минимальным правым идеалом в $\mathfrak{a}$, и обратно).

г) Показать, что если правый цоколь кольца A не содержит минимальных правых идеалов с нулевым квадратом, то всякий правый идеал $\mathfrak{r}$ кольца A, являющийся правым A-модулем конечной длины,

содержится в этом цоколе. (Заметить, что если идемпотент e содержится в $\mathfrak{r}$, то $\mathfrak{r}$ является прямой суммой $e\mathfrak{r}$ и правого аннулятора элемента e в $\mathfrak{r}$; провести индукцию по длине $\mathfrak{r}$.)

*10) Пусть A — примитивное кольцо, плотное подкольцо кольца эндоморфизмов $\mathscr{L}_D(V)$ векторного пространства V над телом D.

а) Кольцо A содержит линейные отображения конечного ранга тогда и только тогда, когда его правый цоколь $\mathfrak{S}$ (упражнение 9) не сводится к 0. (Пусть $\mathfrak{r}$ — минимальный правый идеал кольца A; рассуждая от противного и пользуясь упражнением 8б) и плотностью кольца A, а также существованием проектирования $e \in \mathfrak{r}$ (упражнение 8а) и 5д)), убедиться, что объединение образов $u(V)$, $u \in \mathfrak{r}$ является подпространством размерности 1.) В этом случае цоколь $\mathfrak{S}$ имеет единственное основание (упражнение 5д)).

б) Теперь будем предполагать, что $\mathfrak{S} \neq \{0\}$. Пусть $\mathfrak{r}$ — минимальный правый идеал кольца A. Показать, что элементы $u \in \mathfrak{r}$ могут быть записаны в виде $x \to \langle x, x' \rangle a$, где a не зависят от u и x' пробегает подпространство V' сопряженного к V пространства V^* (использовать плотиость кольца A). Показать, что подпространство V' не зависит от рассматриваемого идеала $\mathfrak{r}$ (см. упражнение 8в)) и соотношение $\langle x, x' \rangle = 0$ для любого $x' \in V'$ влечет $x = 0$ (см. упражнение 5д)). Вывести отсюда, что $\mathfrak{S}$ есть множество эндоморфизмов u пространства V, имеющих конечный ранг, ядра которых $u^{-1}(0)$ являются пересечением конечного числа гиперплоскостей $x_i'^{-1}(0)$, где элементы x_i' принадлежат V' (использовать плотность кольца A). Равенство $A = \mathfrak{S}$ может быть выполнено только в случае, когда V конечномерно и $A = \mathscr{L}_D(V)$.

°в) Наделим V топологией $\sigma_0(V, V')$, согласованной с его структурой абелевой группы и в которой фундаментальная система окрестностей нуля состоит из конечных пересечений гиперплоскостей $x'^{-1}(0)$, где $x' \in V'$. Показать, что всякий эндоморфизм из кольца A непрерывен в этой топологии. Обратно, пусть V' — подпространство в V^* такое, что соотношение $\langle x, x' \rangle = 0$ для всех $x' \in V'$ влечет $x = 0$. Показать, что в кольце $\mathscr{L}_D(V)$ всякое подкольцо A, состоящее из линейных отображений, непрерывных относительно $\sigma_0(V, V')$, и содержащее все линейные отображения конечного ранга, непрерывные относительно $\sigma_0(V, V')$, является примитивным кольцом.

г) Показать, что всякий двусторонний $\neq\{0\}$ идеал кольца A содержит правый цоколь $\mathfrak{S}$.

д) Показать, что кольцо A^0, противоположное A, примитивно и изоморфно кольцу эндоморфизмов пространства V', состоящему из линейных отображений, непрерывных относительно $\sigma_0(V', V)$, и содержащему все линейные отображения конечного ранга, непрерывные относительно $\sigma_0(V', V)$; вывести отсюда, что левый цоколь кольца A равен его правому цоколю.

е) Вывести из б) и д), что примитивное нетерово кольцо с цоколем, не сводящимся к нулю, просто (рассматривая идеалы, содержащиеся

в $\mathfrak{G}$, показать, что пространство V' будет конечномерным) (см. упражнение 13).

ж) Пусть M — подпространство в V^0, имеющее конечную размерность k. Показать, что в $\mathfrak{G}$ существует проектирование e_M пространства V на M. (Рассмотреть в V' ортогональное к M подпространство M^0 — множество элементов $x' \in V'$ таких, что $\langle x, x'\rangle = 0$ для всех $x \in M$; показать, что факторразмерность M^0 в V' равна k; взять в V' дополнение N' к подпространству M^0 и такие базисы (a_i) и (b'_i) в M и N' соответственно, чтобы $\langle a_i, b'_j\rangle = \delta_{ij}$; показать, что $e_M(x) = \sum_i \langle x, b'_i\rangle a_i$ является требуемым проектированием.) Вывести отсюда, что всякий эндоморфизм пространства V, переводящий M на некоторое подпространство в M и равный нулю на ядре $N = N'^0$ проектирования e_M, принадлежит цоколю кольца A (использовать плотность кольца A).

з) Пусть $(u_i)_{1 \geqslant i \geqslant m}$ — конечная последовательность элементов цоколя $\mathfrak{G}$. Показать, что в пространстве V найдутся конечномерное подпространство M и его дополнение N, являющееся пересечением конечного числа гиперплоскостей вида $x'^{-1}(0)$, где $x' \in V'$, такие, что кольцо эндоморфизмов u пространства V, равных нулю на N и удовлетворяющих условию $u(M) \subset M$, содержится в кольце A и содержит все u_i (пусть M_1 — сумма подпространств $u_i(V)$, N_1 — пересечение подпространств $u_i^{-1}(0)$; применить ж) к подпространству $M \supset M_1$ такому, что $M + N_1 = V$, и взять $N' \supset N_1^0$).

11) Пусть A — примитивное кольцо, цоколь которого $\mathfrak{G}$ не сводится к 0. Показать, что A-модуль M тогда и только тогда изотипен, точен и полупрост, когда $\mathfrak{G}M = M$ (заметить, что изоморфные модули имеют одинаковый аннулятор, и применить предложение 5 § 3). Вывести отсюда, что если A-модуль M имеет подмодуль N, который, так же как и фактормодуль M/N, изотипен, точен и полупрост, то модуль M обладает этими свойствами.

*12) Пусть K — поле, V — векторное пространство над K со счетным базисом $(e_n)_{n \geqslant 1}$. Пусть эндоморфизмы u, v пространства V определяются формулами $u(e_1) = 0$, $u(e_n) = e_{n-1}$, $n > 1$, $v(e_n) = e_{n+1}$ для $n \geqslant 1$, и пусть A — подалгебра (над полем K) в $\mathscr{L}_K(V)$, порожденная 1, u и v.

а) Показать, что $uv = 1$, $vu = 1$ и элемеяты $v^i u^j$ $(i \geqslant 0, j \geqslant 0)$ образуют базу алгебры A над K.

б) Вывести отсюда, что кольцо A примитивно и его цоколь есть множество $\mathfrak{G}$ эндоморфизмов w пространства V таких, что $w(e_n) = 0$ для всех n, кроме конечного числа. Показать, что алгебра $A/\mathfrak{G}$ изоморфна подалгебре алгебры $K(X)$, состоящей из рациональных дробей $p(X)/X^m$ ($m \geqslant 0$ — произвольное целое число, $p \in K[X]$).

*13) Пусть K — поле характеристики 0, $E = K(X)$ — поле рациональных дробей от одного переменного над полем K, Ω —кольцо

эндоморфизмов абелевой группы E. Пусть A — подкольцо, порожденное в Ω кольцом умножений поля E и дифференцированием $D = d/dX$ этого поля. Всякий элемент подкольца A однозначно записывается в виде $\sum_{k=0}^{m} a_k D^k$, где $a_k \in E$ (отождествленному со своим кольцом умножений).

а) Показать, что всякий левый или правый идеал кольца A моногенен (рассмотреть в этом идеале элемент $\sum_{k=0}^{m} a_k D^k$, $a_m \neq 0$, для которого m — наибольшее из возможных). Вывести отсюда, что кольцо A нетерово слева и справа, но не имеет минимальных левых и правых идеалов.

б) Показать, что кольцо A квазипросто и без делителей нуля (тем же методом).

в) Показать, что в кольце A найдутся такие элементы u, v, что $uv - vu = 1$. Показать, что в алгебре B конечного ранга над полем K не найдется пары элементов, обладающих этим свойством (рассмотрев B как подкольцо в кольце эндоморфизмов векторного K-пространства B, отождествить B с его кольцом левых умножений; применить предложение 2 гл. III, § 4, n° 5).

*14) Пусть M — свободный моноид с двумя образующими a, b и с единицей, и A — алгебра моноида M над полем K. Показать, что A — примитивное кольцо. Рассуждать следующим образом: пусть V — векторное пространство над полем K, $(e_n)_{n\geqslant 1}$ — счетный базис пространства V, и u и v_2 — эндоморфизмы V, определенные формулами $u(e_1) = 0$, $u(e_n) = e_{n-1}$, $n > 1$, $v_2(e_n) = e_{2n}$, $n \geqslant 1$; рассмотрим гомоморфизм φ_2 алгебры A в $\mathscr{L}_K(V)$, определенный равенствами $\varphi_2(a) = u$, $\varphi_2(b) = v_2$; это определяет на V структуру A-модуля. Показать сначала, что V — простой A-модуль, установив, что для любого $x \in V$ и любого целого $n > 0$ существуют $w_1 \in \varphi_2(A)$ такой, что $w_1(x) = e_1$, и $w_2 \in \varphi_2(A)$ такой, что $w_2(e_1) = e_n$. Затем показать, что A-модуль V точный: обозначим через $P_h(n)$, $h \in M$, индекс s вектора $e_s = \varphi_2(h)(e_n)$. °Показать, что P_h есть функция (H) (Функции действительного переменного, гл. V, приложение) и что если h и k — различные элементы моноида M, то $P_h \neq P_k$ (рассмотреть последовательные логарифмы функции P_h).° Вывести отсюда, что для всякого отличного от нуля элемента c алгебры A существует целое число n такое, что $\varphi_2(c)(e_n) \neq 0$.

Пусть аналогично v_r, $r > 2$, — эндоморфизм пространства V, определенный формулой $v_r(e_n) = e_{rn}$, $n \geqslant 1$. Показать, что гомоморфизм φ_r алгебры A в $\mathscr{L}_K(V)$, определенный равенствами $\varphi_r(a) = u$, $\varphi_r(b) = v_r$, также определяет на V структуру точного простого A-модуля и эти структуры попарно не изоморфны).

15) Пусть A — простое кольцо, M — левый A-модуль, M^* — его сопряженный (гл. II, § 4, n° 1) модуль.

а) Показать, что если модуль M имеет конечную длину n, то M^* — правый A-модуль длины n; вывести отсюда, что кольцо A фробениусово (§ 4, упражнение 10).

б) Для любого подмодуля N модуля M подмодуль N^{00}, ортогональный к модулю N, ортогональному к N, совпадает с N.

в) Обобщить на модули M и M^* теоремы 1, 3 и 4 гл. II, § 4.

16) Пусть A — полупростая алгебра конечного ранга над полем K и A_i $(1 \leqslant i \leqslant r)$ — ее простые компоненты, A_i изоморфна кольцу матриц над телом D_i; обозначим через m_i ранг тела D_i над полем K. Пусть B — полупростая подалгебра в A, содержащая ее единицу, и B_j $(1 \leqslant j \leqslant s)$ — ее простые компоненты, B_j изоморфна кольцу матриц над телом E_j; обозначим через n_j ранг тела E_j над полем K. Пусть $\mathfrak{l}_i$ — минимальный левый идеал в A_i, $\mathfrak{l}'_j$ — минимальный левый идеал в B_j, $\mathfrak{n}_j$ — левый идеал в A, порожденный $\mathfrak{l}'_j$; показать, что $m_i\,[\mathfrak{n}_j : \mathfrak{l}_i] = n_j\,[\mathfrak{l}_i : \mathfrak{l}'_j]$.

17) Пусть A — полупростое кольцо, A_j $(1 \leqslant j \leqslant r)$ — его простые компоненты, B — полупростое подкольцо в A, содержащее его единицу, B_k $(1 \leqslant k \leqslant s)$ — его простые компоненты. Обозначим через $i(A_j, B_k)$ длину A_j-модуля $A_j \otimes_{B_k} P_k$, где P_k — простой B_k-модуль, и через $h(A_j, B_k)$ — длину изотипной компоненты типа P_k B-модуля, полученного сужением до B кольца операторов простого A-модуля N_j, изоморфного минимальному идеалу кольца A.

Пусть M — точный A-модуль и длина $l_B(M)$ конечна. Тогда коммутант B' B-модуля M и коммутант A' A-модуля M полупросты; пусть A'_j $(1 \leqslant j \leqslant r)$ — простые компоненты A', B'_k $(1 \leqslant k \leqslant s)$ — простые компоненты B', причем компонента A'_j отождествлена с коммутантом изотипной компоненты типа M модуля N_j, а компонента B'_k — с коммутантом изотипной компоненты типа M модуля P_k (§ 4, n° 4, предложение 5). Показать, что $i(B'_k, A'_j) = h(A_j, B_k)$, $h(B'_k, A'_j) = i(A_j, B_k)$.

18) Пусть A — алгебра над полем K, B — простая подалгебра, содержащая ее единицу и имеющая конечный ранг над K. Показать, что $[A : B] = [A^0 : B^0]$.

§ 6. Радикал

1. *Произведения идеалов*

Пусть A — кольцо, M — левый A-модуль. Пусть U — подгруппа абелевой группы A, V — подгруппа абелевой группы M. *Произведением* подгрупп U и V в этой главе будет называться *подгруппа* абелевой группы M, порожденная элементами uv,

где $u \in U$, $v \in V$. Произведение подгрупп будет обозначаться через UV. Аналогичное обозначение используется для правых модулей. $\boldsymbol{Z}$-билинейное отображение $(u, v) \to uv$ произведения $U \times V$ в M определяет $\boldsymbol{Z}$-линейное отображение тензорного произведения $U \otimes_{\boldsymbol{Z}} V$ в M, образом которого будет UV; иными словами, UV есть множество конечных сумм $\sum_{i=1}^{n} u_i v_i$, где $u_i \in U$, $v_i \in V$, $1 \leqslant i \leqslant n$ (n произвольно).

Введенное таким образом понятие не совпадает с рассмотренным в гл. I, § 3, n° 1, где UV есть множество элементов вида $uv \in M$, где $u \in U$ и $v \in V$. Для подгрупп U и V обозначение UV в смысле гл. I в этой главе использоваться не будет.

Пусть $(U_\lambda)_{\lambda \in I}$ — семейство подгрупп в A, $(V_\mu)_{\mu \in J}$ — семейство подгрупп в M. Положим $U = \sum_{\lambda \in I} U_\lambda$, $V = \sum_{\mu \in J} V_\mu$. Тогда $U \times V$ будет суммой семейства $(U_\lambda \times V_\mu)_{(\lambda, \mu) \in I \times J}$ и, следовательно,

$$\Big(\sum_{\lambda \in I} U_\lambda\Big)\Big(\sum_{\mu \in J} V_\mu\Big) = \sum_{(\lambda, \mu) \in I \times J} U_\lambda V_\mu.$$

Более общо: пусть $U_1, \ldots, U_n$ — конечное семейство подгрупп в A, V — подгруппа в M; через $U_1 U_2 \ldots U_n V$ обозначается подгруппа, порожденная в M произведениями $u_1 u_2 \ldots u_n v$, где $u_i \in U_i$ $(1 \leqslant i \leqslant n)$ и $v \in V$.

Возьмем, в частности, $M = A_s$; отображение $(U, V) \to UV$ является тогда внутренним законом композиции в множестве подгрупп абелевой группы A; легко проверяется, что для любых трех подгрупп U_1, U_2, U_3 группы A

$$(U_1 U_2) U_3 = U_1 (U_2 U_3),$$

другими словами, этот закон *ассоциативен*; кроме того, для любых подгрупп U_1, U_2 в A и любой подгруппы V в A-модуле M

$$(U_1 U_2) V = U_1 (U_2 V) = U_1 U_2 V.$$

Для любых подгрупп U_1, U_2 в A и гомоморфизма f кольца A в некоторое кольцо A' выполняется равенство $f(U_1 U_2) = f(U_1) f(U_2)$.

Если $\mathfrak{l}$ — левый идеал в кольце A, то для любой подгруппы V в M произведение $\mathfrak{l}V$ является в M подмодулем. В частности, для любой подгруппы U в A $\mathfrak{l}U$ будет левым идеалом кольца A.

Аналогично $U\mathfrak{r}$, где $\mathfrak{r}$ — правый идеал кольца A, будет правым идеалом в A для любой подгруппы U группы A. Произведение $\mathfrak{l}\mathfrak{r}$ любого левого и любого правого идеалов будет, следовательно, двусторонним идеалом.

Отображение $(\mathfrak{a}, \mathfrak{b}) \to \mathfrak{a}\mathfrak{b}$ является ассоциативным внутренним законом композиции в множестве левых идеалов (соответственно правых двусторонних идеалов) кольца A; так же, как и для любого ассоциативного закона, определяется *n-я степень* левого (соответственно правого двустороннего) идеала: $\mathfrak{a}^n = \mathfrak{a}^{n-1}\mathfrak{a}$, $n > 1$; кроме того, полагают $\mathfrak{a}^0 = A$. Тогда $\mathfrak{a}^{n+1} \subset \mathfrak{a}^n$ для любого $n \geqslant 0$. Если $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ — *двусторонние* идеалы в A, то

$$\mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_n \subset \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \ldots \cap \mathfrak{a}_n.$$

Определение 1. *Пусть A — кольцо. Элемент x* (соответственно *идеал $\mathfrak{a}$*) *кольца A называется нильпотентным, если существует целое число $n > 0$ такое, что $x^n = 0$* (соответственно $\mathfrak{a}^n = \{0\}$). *Идеал кольца A, все элементы которого нильпотентны, называется нильидеалом.*

Замечания. 1) Если элемент $x \in A$ нильпотентен, то $1 - x$ обратим. В самом деле, пусть $x^n = 0$ и $y = 1 + x + x^2 + \ldots + x^{n-1}$. Легко проверить, что $y(1 - x) = (1 - x)y = 1$.

2) Идеал $\mathfrak{a}$ нильпотентен тогда и только тогда, когда существует целое $n > 0$ такое, что произведение любых n элементов идеала $\mathfrak{a}$ равно нулю.

3) Нильпотентный идеал, очевидно, является нильидеалом, но обратное, вообще говоря, неверно; нильидеал $\mathfrak{a} \neq \{0\}$ может даже быть таким, что $\mathfrak{a}^2 = \mathfrak{a}$ (упражнение 2).

2. *Радикал модуля*

Определение 2. *Радикалом A-модуля M называется подмодуль, являющийся пересечением всех его максимальных подмодулей, или, что то же самое, множество элементов модуля M, аннулируемых всяким гомоморфизмом модуля M в простой A-модуль. Говорят, что модуль M без радикала, если его радикал — нуль.*

Если, например, $\mathfrak{n}$ — левый идеал кольца A, то утверждение что $A/\mathfrak{n}$ без радикала, равносильно тому, что $\mathfrak{n}$ есть пересечение максимальных левых идеалов.

Может случиться, что в модуле M нет максимальных подмодулей; в этом случае модуль M совпадает со своим радикалом (§ 3, упражнение 8).

До самого конца этой главы радикал A-модуля M мы будем обозначать через $\mathfrak{R}_A(M)$ или $\mathfrak{R}(M)$.

Предложение 1. *Если M — модуль конечного типа, не сводящийся к 0, то $\mathfrak{R}(M) \neq M$.*

Это следует из существования в M максимальных подмодулей (§ 3, предложение 4).

Предложение 2. *Пусть M, N — A-модули и f — гомоморфизм модуля M в N. Тогда $f(\mathfrak{R}(M)) \subset \mathfrak{R}(N)$.*

В самом деле, пусть g — гомоморфизм модуля N в простой модуль; тогда $g \circ f$ аннулируется на $\mathfrak{R}(M)$, так что g аннулируется на $f(\mathfrak{R}(M))$, откуда и следует предложение.

Предложение 3. *Пусть M — A-модуль и N — его подмодуль.*

а) $\mathfrak{R}(N) \subset \mathfrak{R}(M)$.

б) $\mathfrak{R}(M/N) \supset (\mathfrak{R}(M) + N)/N$; *если* $N \subset \mathfrak{R}(M)$, *то* $\mathfrak{R}(M/N) = \mathfrak{R}(M)/N$.

Утверждение а) и первая часть б) немедленно следуют из предложения 2. Вторая часть б) вытекает из существования в случае $N \subset \mathfrak{R}(M)$ взаимно однозначного соответствия между максимальными подмодулями в M и максимальными подмодулями в M/N (гл. I, § 6, n° 13, теорема 6).

Следствие 1. *Радикал модуля M является наименьшим из подмодулей N таких, что M/N без радикала.*

В самом деле, если фактормодуль M/N без радикала, то по первой части предложения 3 $\mathfrak{R}(M) + N = N$, откуда $\mathfrak{R}(M) \subset N$. Обратно, если $N = \mathfrak{R}(M)$, то $\mathfrak{R}(M/N) = \{0\}$ по второй части предложения 3б).

Заметим, что могут существовать такие подмодули $N \supset \mathfrak{R}(M)$, что радикал $\mathfrak{R}(M/N)$ не сводится к 0 (замечание к предложению 8, n° 3).

Следствие 2. *Пусть $(M_\iota)_{\iota \in I}$ — некоторое семейство A-модулей. Радикал произведения $\prod_{\iota \in I} M_\iota$ содержится в произведении радикалов $\mathfrak{R}(M_\iota)$; радикал прямой суммы модулей M_ι равен прямой сумме радикалов $\mathfrak{R}(M_\iota)$.*

В самом деле, пусть N_ι — максимальный подмодуль в M_ι; тогда произведение $N_\iota \times \prod_{\varkappa \neq \iota} M_\varkappa$ будет максимальным подмодулем в $P = \prod_{\iota \in I} M_\iota$; следовательно, $\mathfrak{R}(P)$ содержится в каждом произведении $\mathfrak{R}(M_\iota) \times \prod_{\varkappa \neq \iota} M_\varkappa$, и пересечением этих произведений будет $\prod_{\iota \in I} \mathfrak{R}(M_\iota)$, откуда и следует первое утверждение. Пусть $S \subset P$ — прямая сумма модулей M_ι; аналогично предыдущему можно убедиться, что сумма подмодуля N_ι и модулей $M_\varkappa$ с индексами $\neq \iota$ является максимальным подмодулем в S, так что $\mathfrak{R}(S)$ содержится в (прямой) сумме радикалов $\mathfrak{R}(M_\iota)$; но ввиду предложения 3а) выполняется и обратное включение $\mathfrak{R}(M_\iota) \subset \mathfrak{R}(S)$, $\iota \in I$, откуда следует второе утверждение.

Следствие 3. *Пусть M — A-модуль конечного типа; если его подмодуль P обладает свойством $P + \mathfrak{R}(M) = M$, то $P = M$.*

В самом деле, по предложению 3б) $\mathfrak{R}(M/P) = M/P$; но фактормодуль M/P конечного типа, и из предложения 1 следует равенство $M/P = \{0\}$.

Предложение 4. *Пусть M — A-модуль с конечной системой образующих $(x_i)_{1 \leqslant i \leqslant n}$. Для того чтобы элемент $x \in M$ принадлежал $\mathfrak{R}(M)$, необходимо и достаточно, чтобы при любых $a_i \in A$ $(1 \leqslant i \leqslant n)$ элементы $x_i + a_i x$ $(1 \leqslant i \leqslant n)$ составляли систему образующих модуля M.*

В самом деле, пусть $x \in \mathfrak{R}(M)$, и P — подмодуль, порожденный элементами $x_i + a_i x$. Ясно, что $P + \mathfrak{R}(M) = M$, так что $P = M$ по следствию 3 предложения 3.

Обратно, пусть $x \notin \mathfrak{R}(M)$; тогда в M найдется максимальный подмодуль N такой, что $x \notin N$. Следовательно, $Ax + N = M$; поэтому для всякого индекса i существует такой элемент $a_i \in A$, что $x_i \in -a_i x + N$, откуда $x_i + a_i x \in N$, и элементы $x_i + a_i x$ $(1 \leqslant i \leqslant n)$ не порождают M.

Предложение 5. *Для того чтобы A-модуль M был без радикала, необходимо и достаточно, чтобы он был изоморфен некоторому подмодулю произведения простых A-модулей.*

Пусть модуль M без радикала. Существуют семейство $(S_\iota)_{\iota \in I}$ простых A-модулей и семейство $(f_\iota)_{\iota \in I}$ гомоморфизмов модуля M

в S_ι такие, что пересечение ядер f_ι равно $\{0\}$; отображение $x \to (f_\iota(x))_{\iota \in I}$ является тогда инъективным гомоморфизмом модуля M в $\prod_{\iota \in I} S_\iota$. Обратно, пусть M — подмодуль произведения $\prod_{\iota \in I} S_\iota$ простых модулей; для любого элемента $x \neq 0$ модуля M найдется индекс $\iota \in I$ такой, что $pr_\iota x \neq 0$ и сужение g отображения pr_ι на M является гомоморфизмом модуля M в простой модуль S_ι, причем $g(x) \neq 0$; отсюда следует, что модуль M без радикала.

Следствие. *Всякий полупростой модуль является модулем без радикала.*

3. *Радикал кольца*

Определение 3. *Пусть A — кольцо. Радикалом кольца называется радикал A-модуля A_s, то есть пересечение максимальных левых идеалов кольца A. Говорят, что кольцо A без радикала, если его радикал — нуль.*

До самого конца этой главы мы будем обозначать радикал кольца A через $\mathfrak{R}(A)$.

Предложение 6. *Пусть A — кольцо.*

а) *$\mathfrak{R}(A)$ есть пересечение аннуляторов простых левых A-модулей.*

б) *$\mathfrak{R}(A)$ есть наименьший из аннуляторов полупростых левых A-модулей.*

В самом деле, утверждение, что $x \in A$ принадлежит аннулятору любого простого A-модуля, равносильно тому, что x принадлежит аннулятору любого элемента любого простого A-модуля, то есть (§ 3, n° 1, предложения 2 и 3) принадлежит всем максимальным левым идеалам кольца A; это доказывает а). Ясно, что аннулятор всякого полупростого A-модуля является пересечением аннуляторов простых A-модулей, то есть содержит $\mathfrak{R}(A)$. Наконец, пусть $\mathfrak{G}$ — множество классов простых A-модулей (§ 3, n° 2); прямая сумма $\sum_{\lambda \in \mathfrak{G}} \lambda$ является полупростым модулем, и вследствие а) $\mathfrak{R}(A)$ —его аннулятор; отсюда следует б).

Из предложения 6 вытекает, что радикал $\mathfrak{R}(A)$ является двусторонним идеалом кольца A.

Следствие 1. *Пусть A — кольцо, M — A-модуль. Тогда* $\mathfrak{R}(A)M \subset \mathfrak{R}(M)$.

В самом деле, радикал $\mathfrak{R}(A)$ аннулирует все простые A-модули (предложение 6), и следовательно, всякий гомоморфизм модуля M в простой A-модуль аннулируется на $\mathfrak{R}(A)M$.

Замечание. Заметим, что равенство $\mathfrak{R}(M) = \mathfrak{R}(A)M$ верно не всегда, даже если модуль M конечного типа (см. замечание к предложению 8).

Следствие 2 (лемма Накаяма). *Пусть M — A-модуль конечного типа. Если его подмодуль N обладает свойством $N + \mathfrak{R}(A)M = M$, то $N = M$.*

Это вытекает из следствия 1 предложения 6 и следствия 3 предложения 3 n° 2.

Следствие 3. *Пусть M — A-модуль конечного типа, $\mathfrak{m}$ — правый идеал в кольце A, содержащийся в $\mathfrak{R}(A)$. Если $(A_d/\mathfrak{m}) \otimes_A M = \{0\}$, то $M = \{0\}$.*

В самом деле, тензорное произведение $(A_d/\mathfrak{m}) \otimes_A M$ канонически изоморфно $M/(\mathfrak{m}M)$ (гл. III, приложение II, следствие предложения 4). Предположение, сделанное в следствии, означает тогда, что $M = \mathfrak{m}M$; отсюда $M = \{0\}$ (следствие 2).

Следствие 4. *Пусть M, N — A-модули, u — A-линейное отображение модуля M в N, и $\mathfrak{m}$ — правый идеал кольца A, содержащийся в $\mathfrak{R}(A)$. Если отображение $1 \otimes u : (A_d/\mathfrak{m}) \otimes_A M \to (A_d/\mathfrak{m}) \otimes_A N$ сюръективно и модуль N конечного типа, то отображение u сюръективно.*

В самом деле, $(A_d/\mathfrak{m}) \otimes_A u(M) = (A_d/\mathfrak{m}) \otimes_A N$, следовательно, $(A_d/\mathfrak{m}) \otimes_A (N/u(M)) = \{0\}$, и по следствию 3 $N/u(M) = \{0\}$.

Предложение 7. *Пусть A — кольцо, $\mathfrak{n}$ — его двусторонний идеал. Тогда $\mathfrak{R}(A/\mathfrak{n}) \supset (\mathfrak{R}(A) + \mathfrak{n})/\mathfrak{n}$. Если $\mathfrak{n} \subset \mathfrak{R}(A)$, то $\mathfrak{R}(A/\mathfrak{n}) = \mathfrak{R}(A)/\mathfrak{n}$.*

Это вытекает из предложения 3 и того факта, что модули $A_s/\mathfrak{n}$ и $(A/\mathfrak{n})_s$ имеют одно и то же кольцо гомо етий, то есть одни и те же подмодули и один и тот же радикал.

Следствие. *Радикал кольца A является наименьшим из его двусторонних идеалов $\mathfrak{n}$ таких, что $A/\mathfrak{n}$ без радикала.*

Элемент x кольца A называется *обратимым слева* (соответственно *справа*), если существует $y \in A$ такой, что $yx = 1$ (соответственно $xy = 1$). Элемент y называется тогда *левым* (соответственно *правым*) *обратным* для x. Утверждение, что элемент x обратим слева (соответственно справа), равносильно тому, что x является образующим модуля A_s (соответственно A_d).

Теорема 1. *Пусть A — кольцо. Для того чтобы элемент $x \in A$ принадлежал $\mathfrak{R}(A)$, необходимо и достаточно, чтобы при любом $a \in A$ элемент $1 - ax$ был обратим слева.*

Так как 1 является образующим модуля A_s, то утверждение теоремы немедленно следует из предложения 4.

Следствие 1. *Радикал $\mathfrak{R}(A)$ является наибольшим из двусторонних идеалов $\mathfrak{a}$ таких, что элемент $1 - ax$ обратим при всех $a \in \mathfrak{a}$.*

Ввиду теоремы 1 достаточно показать, что элемент $1 - x$ обратим при всех $x \in \mathfrak{R}(A)$. Пусть $y \in A$ и $y(1 - x) = 1$; тогда $z = 1 - y = -yx \in \mathfrak{R}(A)$ и, следовательно, найдется $y' \in A$ такой, что $1 = y'(1 - z) = y'y$. Таким образом, элемент y обратим (гл. I, § 2, n° 3, предложение 4) и элемент $1 - x = y^{-1}$ также обратим.

Следствие 2. *Пусть A^0 — кольцо, противоположное к A. Тогда $\mathfrak{R}(A^0) = \mathfrak{R}(A)$.*

Это сразу вытекает из следствия 1.

Из этого следствия получается, что $\mathfrak{R}(A)$ является *пересечением максимальных правых идеалов кольца A.*

Следствие 3. *Всякий нильидеал (левый или правый) кольца A содержится в $\mathfrak{R}(A)$.*

Пусть $\mathfrak{n}$ — левый нильидеал кольца A и $x \in \mathfrak{n}$. Элемент ax при любом $a \in A$ принадлежит идеалу $\mathfrak{n}$, то есть нильпотентен; отсюда следует, что элемент $1 - ax$ обратим (n° 1, замечание 1); поэтому $x \in \mathfrak{R}(A)$. Для правых идеалов утверждение доказывается переходом к кольцу A^0.

Замечание. Нильпотентный элемент кольца A может не входить в $\mathfrak{R}(A)$: это видно из примера, где A — кольцо матриц $M_r(D)$ над телом (см. § 5, n° 4, теорема 2). В то же время всякий нильпотентный элемент *центра* кольца A порождает нильпотентный дву-

сторонний идеал и, следовательно, принадлежит $\mathfrak{R}(A)$. С другой стороны, радикал $\mathfrak{R}(A)$ не обязательно является нильидеалом (см. ниже пример 1); тем более $\mathfrak{R}(A)$ не обязан быть нильпотентным идеалом; может случиться, что $(\mathfrak{R}(A))^2 = \mathfrak{R}(A)$, хотя все элементы его нильпотентны (упражнение 2).

Следствие 4. *Радикал произведения семейства колец* $(A_\iota)_{\iota\in I}$ *равен произведению радикалов* $\mathfrak{R}(A_\iota)$.

В самом деле, в произведении $\prod_{\iota\in I} A_\iota$ обратимы слева те элементы, проекции которых на каждое A_ι обратимы слева.

Теорема 2. *Пусть* A *— кольцо,* $\mathfrak{l}$ *— его левый идеал. Включение* $\mathfrak{l} \subset \mathfrak{R}(A)$ *выполняется тогда и только тогда, когда* $\mathfrak{l}M \neq M$ *для любого* A*-модуля* M *конечного типа, не сводящегося к* 0.

Если модуль M конечного типа и $\neq \{0\}$, то $\mathfrak{R}(M) \neq M$ (n° 2, предложение 1); следовательно, при $\mathfrak{l} \subset \mathfrak{R}(A)$ и $\mathfrak{l}M \neq M$ (следствие 1 предложения 6). Обратно, если для любого A-модуля $M \neq \{0\}$ конечного типа $\mathfrak{l}M \neq M$, то, в частности, для простого A-модуля S будем иметь $\mathfrak{l}S = \{0\}$, то есть $\mathfrak{l} \subset \mathfrak{R}(A)$ (предложение 6).

Примеры. 1) Кольцо A формальных степенных рядов от p переменных с коэффициентами из поля K является кольцом целостности (гл. IV, § 5, n° 3, теорема 1); его обратимыми элементами являются формальные ряды со свободным членом $\neq 0$ (гл. IV, § 5, n° 6, предложение 4). Формальные ряды без свободного члена составляют в A единственный максимальный идеал, то есть радикал кольца A. Единственным нильпотентным элементом радикала является 0.

°Более общее утверждение: радикал локального кольца является его единственным максимальным идеалом.°

Заметим, что поле дробей кольца A без радикала, так что подкольцо кольца без радикала может иметь радикал $\neq \{0\}$.

2) Пусть C — кольцо целостности; всякое кольцо многочленов $A = C[X_\iota]_{\iota\in I}$, где множество I непусто, является кольцом без радикала. В самом деле, пусть $f \in A$ и $f \neq 0$; тогда многочлен $1 - fg$ при любом $g \in A$ степени > 0 будет иметь степень > 0 и, следовательно, необратим в A.

Заметим, что если $B = K[[X_1, \ldots, X_p]]$, где K — поле, и $A = K[X_1, \ldots, X_p]$ — подкольцо в B, то $\mathfrak{R}(A) = \{0\}$, а $A \cap \mathfrak{R}(B) \neq \{0\}$ (см. пример 1).

3) Пусть E — множество, K — поле, A — кольцо функций, определенных в E и принимающих значения в K, содержащее все константные функции. Кольцо A без радикала. В самом деле, отображение $f \to f(x)$ при любом $x \in E$ является гомоморфизмом кольца A на K, так что его ядро является в A максимальным идеалом $\mathfrak{m}_x$; пересечение всех $\mathfrak{m}_x$, очевидно, равно $\{0\}$.

Предложение 8. *Пусть A — кольцо главных идеалов.*

а) *Кольцо A без радикала тогда и только тогда, когда A тело или множество максимальных идеалов A бесконечно.*

б) *Факторкольцо A/Ax без радикала тогда и только тогда, когда элемент x не делится ни на какую степень экстремального элемента с показателем > 1 (или, как говорят еще, допуская вольность речи, x не имеет кратных множителей* *)).

Пусть (p_α)— система представителей экстремальных элементов. Максимальными в A являются идеалы Ap_α; для того чтобы элемент $z \in A$ принадлежал $\mathfrak{R}(A)$, необходимо и достаточно, чтобы он делился на все p_α, откуда следует а). Пусть $x = u \prod_\alpha p_\alpha^{n_\alpha}$— разложение элемента x на экстремальные элементы; кольцо A/Ax изоморфно тогда произведению колец $A/Ap_\alpha^{n_\alpha}$ (гл. VII, § 1, n° 2, предложение 4). Если все n_α равны 1, то кольца A/Ap_α являются полями и кольцо A/Ax полупросто. С другой стороны, идеалы кольца $A/Ap_\alpha^{n_\alpha}$ являются каноническими образами идеалов Ap_α^m, $0 \leqslant m \leqslant n$. Таким образом, при $n_\alpha > 1$ радикал кольца $A/Ap_\alpha^{n_\alpha}$ равен $Ap_\alpha/Ap_\alpha^{n_\alpha}$, и следовательно, факторкольцо A/Ax имеет ненулевой радикал.

Замечание. Положив $A = \boldsymbol{Z}$, получаем, что факторкольцо кольца без радикала может иметь радикал, отличный от нуля. Кроме того, для любого $\boldsymbol{Z}$-модуля M выполняется равенство $\mathfrak{R}(\boldsymbol{Z})\, M = \{0\}$, хотя радикал модуля M может быть отличен от $\{0\}$ (например, при $M = \boldsymbol{Z}/(p^n)$, где p — простое число, $n > 1$).

*) Вольность состоит в том, что всякий элемент кольца A делится на любую степень любой *единицы* кольца A.

4. Радикал артинова кольца и артинова модуля

Теорема 3. *Радикал артинова кольца A является наибольшим нильпотентным двусторонним идеалом кольца A.*

Всякий нильпотентный двусторонний идеал кольца A содержится в $\mathfrak{R} = \mathfrak{R}(A)$ (n° 3, следствие 3 теоремы 1). Надо доказать, следовательно, что $\mathfrak{R}$ нильпотентен. Последовательность $\mathfrak{R}^n$ убывает, так что существует такое целое p, что $\mathfrak{R}^p = \mathfrak{R}^{p+1} = \ldots$ $\ldots = \mathfrak{a}$. Предположим, что $\mathfrak{a} \neq \{0\}$. Существуют такие левые идеалы $\mathfrak{l}$, что $\mathfrak{a}\mathfrak{l} \neq \{0\}$, например $\mathfrak{l} = \mathfrak{R}$. Пусть $\mathfrak{m}$ — минимальный элемент множества таких левых идеалов. Имеем $\mathfrak{a}(\mathfrak{R}\mathfrak{m}) = (\mathfrak{a}\mathfrak{R})\,\mathfrak{m} = \mathfrak{a}\mathfrak{m} \neq \{0\}$; так как $\mathfrak{R}\mathfrak{m} \subset \mathfrak{m}$, то, по определению $\mathfrak{m}$, $\mathfrak{R}\mathfrak{m} = \mathfrak{m}$. Доказав теперь, что A — модуль $\mathfrak{m}$ конечного типа, мы получим отсюда противоречие (n° 3, теорема 2). Однако, по предположению, найдется элемент $x \in \mathfrak{m}$ такой, что $\mathfrak{a}x \neq \{0\}$; следовательно, $\mathfrak{a}(Ax) \neq \{0\}$; поскольку $Ax \subset \mathfrak{m}$, то, по определению $\mathfrak{m}$, $Ax = \mathfrak{m}$, что и заканчивает доказательство.

Следствие. *Радикал коммутативного артинова кольца является множеством его нильпотентных элементов.*

Теорема 4. *Для того чтобы модуль M был полупростым и конечной длины, необходимо и достаточно, чтобы он был артиновым и без радикала.*

Уже известно, что полупростой модуль конечной длины артинов (§ 2, n° 1, предложение 3) и без радикала (n° 2, следствие предложения 5). Обратно, пусть M — артинов модуль без радикала, и $\mathfrak{R}$ — минимальный элемент множества конечных пересечений максимальных подмодулей модуля M. Если N — максимальный подмодуль в M, то $N \cap R \subset R$, откуда по определению R, $N \cap R = R$, то есть $R \subset N$. Отсюда, ввиду $\mathfrak{R}(M) = \{0\}$, следует, что $R = \{0\}$. Следовательно, в M существует конечное семейство максимальных подмодулей M_i $(1 \leqslant i \leqslant n)$, пересечение которых равно $\{0\}$. Отображение $x \to (f_i(x))$, где f_i — канонический гомоморфизм модуля M на M/M_i, является инъективным гомоморфизмом модуля M в $\prod_{i=1}^{n} (M/M_i) = P$; но модуль P

полупрост и имеет конечную длину; следовательно, модуль M также полупрост и имеет конечную длину.

Следствие 1. *Фактормодуль артинова модуля по его радикалу является полупростым модулем конечной длины.*

В самом деле, этот фактормодуль артинов (§ 2, n° 1, предложение 2) и без радикала (n° 2, следствие 1 предложения 3).

Следствие 2. *Для того чтобы кольцо было полупростым, необходимо и достаточно, чтобы оно было артиновым и без радикала.*

В самом деле, если кольцо A полупросто, то модуль A имеет конечную длину (§ 4, n° 1, замечание).

Следствие 3. *Факторкольцо артинова кольца по его радикалу полупросто.*

В самом деле, модули $A_s/\mathfrak{R}(A)$ и $(A/\mathfrak{R}(A))_s$ имеют одно и то же кольцо гомотетий и, следовательно, одни и те же подмодули; поэтому утверждение вытекает из следствия 1.

Следствие 4. *Для того чтобы кольцо A было простым, необходимо и достаточно, чтобы оно было артиновым и единственными его двусторонними идеалами были $\{0\}$ и A.*

Известно уже, что эти условия необходимы. Они и достаточны, так как при их выполнении $\mathfrak{R}(A) = \{0\}$, то есть кольцо A полупросто (следствие 2) и, по определению (§ 5, n° 2, определение 2), просто.

Предложение 9. *Пусть A — коммутативное кольцо. Следующие утверждения эквивалентны:*

а) *Кольцо A артиново и не содержит нильпотентных элементов $\neq 0$.*

б) *Кольцо A полупросто.*

в) *Кольцо A — прямая композиция конечного числа полей.*

Согласно следствию теоремы 3 утверждение а) равносильно тому, что кольцо A артиново и без радикала; следовательно, эквивалентность а) и б) является частным случаем следствия 2 теоремы 4. Эквивалентность б) и в) вытекает из предложения 12 и теоремы 2 § 5, n° 4.

Следствие. *Всякая подалгебра конечного ранга* коммутативной *алгебры без радикала над полем K является прямой композицией конечного числа полей, каждое из которых является расширением конечной степени поля K.*

В самом деле, всякая такая подалгебра является артиновым кольцом и не содержит нильпотентных элементов $\neq 0$ (замечание к следствию 3 теоремы 1).

5. *Модули над артиновым кольцом*

Предложение 10. *Пусть A — артиново кольцо, M — A-модуль. Следующие свойства эквивалентны:*

а) *Модуль M полупрост;*

б) $\mathfrak{R}(A)\,M = \{0\}$;

в) *Кольцо гомотетий A_M полупросто.*

В самом деле, всякий модуль над полупростым кольцом полупрост (§ 5, n° 1, определение 1), так что из в) следует а); аннулятор любого полупростого A-модуля содержит $\mathfrak{R}(A)$ (n° 3, предложение 6), так что из а) следует б); на конец, из б) следует в), так как равенство $\mathfrak{R}(A)\,M = \{0\}$ влечет, что кольцо A_M изоморфно факторкольцу $A/\mathfrak{R}(A)$; это факторкольцо полупросто (n° 4, следствие 3 теоремы 4), так что кольцо A_M также полупросто (§ 5, n° 3, предложение 10).

Предложение 11. *Пусть A — артиново кольцо. Существует лишь конечное число классов простых A-модулей, и оно равно числу простых компонент факторкольца $A/\mathfrak{R}(A)$.*

Из определения радикала следует, что всякий простой A-модуль можно рассматривать как простой $(A/\mathfrak{R}(A))$-модуль, и наоборот. Но кольцо $A/\mathfrak{R}(A)$ полупросто (n° 4, следствие 3 теоремы 4), так что достаточно применить предложение 11, § 5, n° 3.

Предложение 12. *Пусть кольцо A обладает таким нильпотентным двусторонним идеалом* n, *что $A/\mathfrak{n}$ полупросто (например, A — артиново кольцо) и M — произвольный A-модуль. Следующие три свойства эквивалентны:*

а) *M имеет конечную длину;*

б) *M артинов;*

в) *M нетеров.*

Известно, что а) влечет б) и в) (§ 2, n° 1, предложение 3). Предположим теперь, что модуль M артинов (соответственно нетеров) и $\mathfrak{n}^p = \{0\}$. Достаточно показать, что модули $M/\mathfrak{n}M$, $\mathfrak{n}M/\mathfrak{n}^2M$, . . ., $\mathfrak{n}^{p-1}M/\mathfrak{n}^p M$ имеют конечную длину. Однако эти модули аннулируются идеалом $\mathfrak{n}$, то есть их можно рассматривать как $(A/\mathfrak{n})$-модули, и притом полупростые $(A/\mathfrak{n})$-модули. Так как они, сверх того, артиновы (соответственно нетеровы) (§ 2, n° 1, предложение 2), то наше утверждение доказано (§ 2, n° 1, пример 2).

Следствие 1. *Пусть A — артиново кольцо, M — A-модуль конечного типа. Тогда модуль M имеет конечную длину.*

В самом деле, модуль M артинов (§ 2, n° 3, предложение 7).

Следствие 2. *Для любого артинова кольца A модуль A_s имеет конечную длину.*

Это утверждение — частный случай следствия 1.

Следствие 3. *Всякое артиново кольцо нетерово.*

Предложение 13. *Пусть A — коммутативная алгебра конечного ранга над алгебраически замкнутым полем K.*

Всякий простой A-модуль имеет над K размерность 1.

Всякий простой A-модуль можно рассматривать как простой модуль над кольцом $A/\mathfrak{R}(A)$; следовательно, можно ограничиться случаем, когда кольцо A полупросто. Тогда всякий простой A-модуль является простым модулем над одной из простых компонент кольца A (§ 5, n° 3, предложение 11). Но кольцо A коммутативно, а поле K алгебраически замкнуто, так что простые компоненты кольца A являются полями, изоморфными K (n° 4, следствие предложения 9); отсюда и следует утверждение.

Упражнения. 1) Привести пример ненулевых идеалов $\mathfrak{a}$, $\mathfrak{b}$, с кольца $\boldsymbol{Z}$, для которых $\mathfrak{ab} \neq \mathfrak{a} \cap \mathfrak{b}$ и $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) \neq \mathfrak{a} + \mathfrak{bc}$.

2) Пусть p — простое число, U_p — p-компонента группы $\boldsymbol{Q}/\boldsymbol{Z}$ (гл. VII, § 2, упражнение 3б)). Пусть A — (коммутативная) алгебра группы U_p (записываемая мультипликативно) над простым полем $\boldsymbol{F}_p$. Показать, что $\mathfrak{R}(A)$ — единственный максимальный идеал в A и порождается элементами $1 - s$, где s пробегает U_p; $\mathfrak{R}(A)$ является нильидеалом, и $(\mathfrak{R}(A))^2 = \mathfrak{R}(A)$.

3) а) Пусть $\mathfrak{l}$ — нильпотентный левый идеал кольца A. Показать, что двусторонний идеал $\mathfrak{l}A$, порожденный идеалом $\mathfrak{l}$, нильпотентен.

б) Показать, что сумма двух двусторонних нильидеалов (соответственно двусторонних нильпотентных идеалов) будет нильидеалом (соответственно нильпотентным идеалом).

в) Показать, что сумма $\mathfrak{U}$ всех двусторонних нильидеалов является нильидеалом, а сумма $\mathfrak{N}$ всех нильпотентных двусторонних нильидеалов является нильидеалом, содержащим все нильпотентные (левые и правые) идеалы.

г) Двусторонний идеал $\mathfrak{a}$ кольца A называется *нильрадикалом*, если $\mathfrak{a}$ — нильидеал и факторкольцо $A/\mathfrak{a}$ не содержит нильпотентных идеалов. Показать, что $\mathfrak{U}$ — максимальный нильрадикал кольца A; если A коммутативно, то $\mathfrak{U} = \mathfrak{N}$.

д) Пусть I — множество порядковых чисел α (Теор. мн., гл. III, § 2, упражнение 13) таких, что Card $(\alpha) \leqslant$ Card (A). С помощью трансфинитной индукции для любого $\alpha \in I$ следующим образом определим двусторонний идеал $\mathfrak{N}_\alpha$ кольца A: $\mathfrak{N}_0 = \mathfrak{N}$; если число α имеет предшествующее $\alpha - 1$, то $\mathfrak{N}_\alpha$ — двусторонний идеал такой, что $\mathfrak{N}_\alpha/\mathfrak{N}_{\alpha-1}$ является суммой нильпотентных идеалов факторкольца $A/\mathfrak{N}_{\alpha-1}$; в противном случае $\mathfrak{N}_\alpha$ — объединение всех $\mathfrak{N}_\beta$, $\beta < \alpha$. Пусть τ — наименьшее порядковое число, для которого $\mathfrak{N}_{\tau+1} = \mathfrak{N}_\tau$, и пусть $\mathfrak{C} = \mathfrak{N}_\tau$. Показать, что $\mathfrak{C}$ — наименьший нильрадикал кольца A и является пересечением всех двусторонних идеалов $\mathfrak{a}$, для которых $A/\mathfrak{a}$ не имеет нильпотентных идеалов *).

4) Пусть A — кольцо.

а) Показать, что $Z \cap \mathfrak{N}(A)$, где Z — центр кольца A, содержится в $\mathfrak{N}(Z)$ (см. упражнение 9б)).

б) Показать, что $\mathfrak{N}(A)$ не имеет ненулевых идемпотентов.

в) Показать, что пересечение радикала $\mathfrak{N}(A)$ с правым цоколем $\mathfrak{S}$ кольца A (§ 5, упражнение 9) равно пересечению $\mathfrak{S}$ с его правым аннулятором в A и является двусторонним идеалом с нулевым квадратом (использовать упражнения 8 и 9а) § 5).

г) Пусть e — идемпотент кольца A. Показать, что радикал кольца eAe равен $e\mathfrak{N}(A)e$ (заметить, что при $a \in eAe$ $(1 - a)(1 - e) = (1 - e)(1 - a) = 1 - e$).

5) Пусть A — кольцо. Показать, что радикал кольца матриц $\boldsymbol{M}_n(A)$ совпадает с идеалом $\boldsymbol{M}_n(\mathfrak{N}(A))$ (см. § 1, упражнения 3 и 9).

*6) Пусть A — коммутативное кольцо, $B = A[X]$ — кольцо многочленов от одного переменного над кольцом A.

а) Предположим сначала, что кольцо A не имеет нильпотентных элементов. Пусть $f = \sum_k a_k X^k$, $g = \sum_k b_k X^k$ — элементы кольца B, и в многочлене fg все члены степени $\geqslant m$ равны нулю. Показать, что $a_p b_q = 0$ при $p + q \geqslant m$.

---

*) Пример кольца, в котором $\mathfrak{C} \neq \mathfrak{U}$, см. R. Baer, Radical ideals, Amer. Journ. of Math., t. LXV (1943), p. 540.

б) Пусть $\mathfrak{N}$ — нильрадикал кольца A (упражнение 3г)). Показать, что многочлен $f \in B$ обратим в кольце B тогда и только тогда, когда его свободный член обратим в A, а все остальные коэффициенты принадлежат $\mathfrak{N}$ (применить к коэффициентам многочлена f канонический гомоморфизм кольца A на $A/\mathfrak{N}$ и воспользоваться упражнением а)).

в) Вывести из б), что радикал кольца B есть идеал $\mathfrak{N}[X]$ и совпадает с нильрадикалом кольца B.

7) а) Для того чтобы кольцо A было без радикала, необходимо и достаточно, чтобы оно было изоморфно некоторому подкольцу C произведения $B = \prod_{\iota \in I} B_\iota$ примитивных колец B_ι (§ 5, упражнение 5), содержащему единицу кольца B и такому, что $pr_\iota(C) = B_\iota$ для всех $\iota \in I$ (рассмотреть множество классов простых A-модулей).

б) Пусть V — векторное пространство бесконечной размерности над телом D, $B = \mathscr{L}_D(V)$ — кольцо его эндоморфизмов, $\mathfrak{S}$ — цоколь кольца B (§ 5, упражнение 10). Рассмотрим в кольце $B \times B$ подкольцо C, порожденное произведением $\mathfrak{S} \times \mathfrak{S}$ и единичным элементом. Показать, что кольцо C без радикала, но не изоморфно произведению примитивных колец.

8) Пусть G — абелева группа без кручения (записываемая мультипликативно), и $K^{(G)}$ — ее алгебра над полем K (гл. II, § 7, n° 9). Показать, что алгебра $K^{(G)}$ без радикала. (Прежде всего, наделить G структурой совершенного порядка, согласованной с ее структурой группы (см. гл. VI, § 1, упражнение 20).)

9) Пусть V — векторное пространство бесконечной размерности над телом D, прямая сумма некоторой последовательности $(V_k)_{k \geqslant 0}$ векторных подпространств одной и той же размерности n; пусть $(e_{ki})_{1 \leqslant i \leqslant n}$ — базис в V_k, и B — некоторое подкольцо кольца матриц $\boldsymbol{M}_n(D^0)$, содержащее единичную матрицу. Рассмотрим множество A эндоморфизмов u пространства V, обладающее свойствами: 1° существует целое число m (зависящее от u) такое, что при $k > m$, сужение эндоморфизма u на V_k является эндоморфизмом пространства V_k, матрица которого относительно базиса (e_{ki}) не зависит от k и принадлежит B; 2° $u(E_m) \subset E_m$, где $E_m = \sum_{k \leqslant m} V_k$.

а) Показать, что A — примитивное кольцо с ненулевым цоколем, состоящим из таких эндоморфизмов $u \in A$, что $u(V_k) = \{0\}$ для всех индексов k, кроме конечного числа (§ 5, упражнение 10).

б) Выбрав подходящим образом D, n и B, привести пример примитивного кольца, факторкольцо которого имеет нильпотентный радикал $\neq \{0\}$, и пример примитивного кольца, центр которого имеет радикал $\neq \{0\}$.

*10) а) Пусть A — кольцо, и его радикал $\mathfrak{R}(A)$ — нильидеал. Пусть $c^2 - c = r \in \mathfrak{R}(A)$, $c \in A$. Показать, что существует такой многочлен f с целыми рациональными коэффициентами, что элемент

$e = c + (2c - 1) f(r)$ идемпотентен. (Заметить, что элемент $(2c - 1)^2$ обратим и обратный к нему имеет вид $g(r)$, где g — многочлен с целыми рациональными коэффициентами; показать затем, что для всякого $t \in \Re(A)$ найдется многочлен h с целыми рациональными коэффициентами такой, что $x = h(t)$ удовлетворяет уравнению $x^2 + x = t$ *(«развернуть» $(1 + 4t)^{1/2}$ по формуле бинома).)*

б) Пусть (u_n) — последовательность элементов кольца $A/\Re(A)$ таких, что $u_i u_j = \delta_{ij} u_j$ для любых индексов i, j. Показать, что в кольце A существует такая последовательность (e_n) ортогональных идемпотентов, что u_n является классом e_n по mod $\Re(A)$. (Использовать а) и заметить, что правый (соответственно левый) аннулятор любого идемпотента $e' \in A$ есть $(1 - e')A$ (соответственно $A(1 - e')$); если, кроме того, $ce' = 0$ (соответственно $e'c = 0$) (обозначения из упражнения а)), то $ee' = 0$ (соответственно $e'e = 0$).)

в) Пусть K — поле, L — несчетное множество индексов, A — алгебра над K, базис которой состоит из единицы e_0, семейства $(c_\lambda)_{\lambda \in L}$ и семейства $(r_{\lambda\mu})_{(\lambda,\mu) \in L \times L}$, а таблица умножения имеет вид

$$c_\lambda^2 = c_\lambda,\ c_\lambda c_\mu = r_{\lambda\mu} \text{ при } \lambda \neq \mu,\ c_\lambda r_{\mu\nu} = \delta_{\lambda\mu} r_{\mu\nu},$$
$$r_{\lambda\mu} c_\nu = \delta_{\mu\nu} r_{\lambda\mu},\ r_{\lambda\mu} r_{\nu\rho} = 0.$$

Показать, что $\Re(A)$ есть подалгебра кольца A с базисом $(r_{\lambda\mu})$, $(\Re(A))^2 = \{0\}$, и в кольце A не существует такого семейства $(e_\lambda)_{\lambda \in L}$ ортогональных идемпотентов, что c_λ сравнимо с e_λ по mod $\Re(A)$ для любого $\lambda \in L$. (Для каждого $\lambda \in L$ рассмотреть множество H_λ элементов $\mu \in L$ таких, что $c_\lambda (e_\mu - c_\mu) = 0$, и показать, что дополнение H_λ в L должно быть конечным, но ни один элемент из L не может принадлежать бесконечно многим множествам H_λ.)

11) Пусть e_1, e_2 — идемпотенты в кольце A, и u_1, u_2 — их канонические образы в кольце $B = A/\Re(A)$. Показать, что если B-модули Bu_1 и Bu_2 изоморфны, то A-модули Ae_1 и Ae_2 изоморфны (пусть $x \in e_1 A e_2$, $y \in e_2 A e_1$ и $xy - e_1 \in \Re(A)$, $yx - e_2 \in \Re(A)$ (§ 1, упражнение 3г)); заметить, что элемент xy обратим в $e_1 A e_1$ (упражнение 5г)); если $xye_1ze_1 = e_1$, рассмотреть элемент $y' = ey_1ze_1$ и показать, что $e_2 - y'x$ — идемпотент (упражнение 5г))).

12) Пусть A — алгебра над полем K и выполняются следующие условия: 1° $\Re(A)$ — нильидеал; 2° $A/\Re(A)$ — прямая композиция конечного числа матричных колец *над полем* K. Показать, что в алгебре A существует такая подалгебра S, что векторное пространство A (над K) является прямой суммой S и $\Re(A)$ (использовать упражнения 10 и 11, а также упражнение 9 § 1).

*13) Кольцо A называется *кольцом Цорна*, если всякий его левый идеал, не являющийся нильидеалом, содержит идемпотент $\neq 0$.

а) Показать, что всякий правый идеал кольца Цорна, не являющийся нильидеалом, содержит идемпотент $\neq 0$ (заметить, что для

любого не нильпотентного элемента $a \in A$ существует $x \in A$ такой, что $xaxa = xa \neq 0$).

б) Показать, что радикал кольца Цорна является нильидеалом.

в) Показать, что кольцо Цорна без делителей нуля — тело.

г) Показать, что примитивное кольцо, цоколь которого (§ 5, упражнение 10) не сводится к 0, является кольцом Цорна (см. § 5, упражнения 5д) и 8а)). Привести пример примитивного кольца, не являющегося кольцом Цорна (см. § 5, упражнение 13), и пример примитивного кольца, у которого цоколь $\neq \{0\}$, но центр не является кольцом Цорна (методом упражнения 9).

д) Пусть K — поле и A — подкольцо произведения $(K(X))^N$, состоящее из последовательностей $s = (f_n)$ таких, что, начиная с некоторого места (зависящего от s), f_n равно одному и тому же элементу $\varphi(s)$ кольца многочленов $K[X]$. Показать, что A — коммутативное кольцо Цорна без радикала, содержащее необратимые элементы, не являющиеся делителями нуля, но его образ $\varphi(A)$ не является кольцом Цорна.

*14) Кольцо A называется *псевдорегулярным*, если для любого $a \in A$ существуют целое число $n > 0$ и элемент $x \in A$ (зависящие от a) такие, что $a^n x a^n = a^n$.

а) Показать, что псевдорегулярное кольцо является кольцом Цорна (упражнение 13), в котором всякий необратимый элемент является левым и правым делителем нуля.

б) Показать, что факторкольцо псевдорегулярного кольца псевдорегулярно (см. упражнение 13д)).

в) Показать, что центр Z псевдорегулярного кольца A является псевдорегулярным кольцом (показать, что если $a^n x a^n = a^n$, где $a \in Z$ и $x \in A$, то $a^{2n}x^k \in Z$ при любом $k \geqslant 1$).

г) Показать, что кольцо A, определенное в упражнении 2, псевдорегулярно, но произведение A^N не псевдорегулярно.

д) Пусть A — псевдорегулярное кольцо; для любого простого числа p p-компонента A_p аддитивной группы A (гл. VII, § 2, n° 2) является в кольце A идеалом, либо равным нулю, либо содержащим идемпотент из центра Z кольца A. (Пусть ε — единица кольца A; используя в), заметить, что если элемент $p\varepsilon$ не нильпотентен, то найдется такой элемент $x \in Z$, что $(p\varepsilon)^n x (p\varepsilon)^n = (p\varepsilon)^n$ для некоторого числа n.) Вывести отсюда, что если кольцо A удовлетворяет, кроме того, условиям упражнения 7а) § 2, то оно будет прямой суммой некоторого (конечного) числа компонент A_p и некоторой алгебры над полем Q рациональных чисел *).

*15) Кольцо A называется *регулярным*, если для любого $a \in A$ существует элемент $x \in A$ такой, что $axa = a$.

а) Для того чтобы кольцо A было регулярным, необходимо и достаточно, чтобы всякий его моногенный левый идеал Aa обладал

*) Упражнение 14д) сообщил нам И. Капланский.

в A_s дополнением или (что то же самое) порождался некоторым идемпотентом.

б) Показать, что сумма двух моногенных идеалов регулярного кольца A является моногенным идеалом (свести доказательство к случаю суммы $Ae_1 + Ae_2$, где e_1, e_2 — идемпотенты и $e_2e_1 = 0$, и рассмотреть элемент $e = e_1 + e_2 - e_1e_2$). Вывести отсюда, что пересечение двух моногенных левых идеалов является моногенным левым идеалом (рассмотреть левые аннуляторы этих идеалов).

в) Факторкольцо регулярного кольца регулярно; любое произведение регулярных колец регулярно.

г) Показать, что всякое регулярное кольцо есть кольцо без радикала (см. упражнение 4б)); вывести отсюда, что всякий двусторонний идеал кольца A является пересечением максимальных левых идеалов, содержащих его.

д) Показать, что центр регулярного кольца регулярен (см. упражнение 14в)).

е) Показать, что кольцо эндоморфизмов векторного пространства регулярно (см. § 5, упражнение 3).

*16) а) Пусть A — регулярное кольцо (упражнение 15). Показать, что в модуле A_s^n всякий подмодуль M конечного типа обладает дополнением (используя упражнение 15б), провести индукцию по n: заметить, что проекция N подмодуля M на первый множитель в A_s^n является моногенным левым идеалом, и вывести отсюда, что модуль $M \cap A_s^{n-1}$ конечного типа; затем рассмотреть дополнение N в A и дополнение $M \cap A_s^{n-1}$ в A_s^n).

б) Вывести из а), что если кольцо A регулярно, то всякое кольцо матриц $M_r(A)$ регулярно (см. § 1, упражнение 9).

*17) а) Пусть кольцо A не имеет нильпотентных элементов $\neq 0$. Показать, что всякий идемпотент $e \in A$ лежит в его центре (рассмотреть элементы $(1 - e)xe$ и $ex(1 - e)$).

б) Пусть A — регулярное кольцо (упражнение 15), не имеющее нильпотентных элементов $\neq 0$. Показать, что для любого $a \in A$, отличного от нуля, найдется элемент $x \in A$ такой, что $e = ax = xa$ — идемпотент (лежащий в центре кольца A) и $ea = ae = a$, вывести отсюда, что для любого $y \in A$ существует $z \in A$ такой, что $ya = az$, и, следовательно, всякий левый или правый идеал кольца A является двусторонним.

в) В предположениях упражнения б) показать, что всякое факторкольцо кольца A регулярно и не имеет нильпотентных элементов $\neq 0$ (использовать б)). Вывести отсюда, что кольцо A изоморфно некоторому подкольцу C произведения $B = \prod_{\iota \in I} D_\iota$ тел D_ι, содержащему единицу B и такому, что $pr_\iota(C) = D_\iota$ для любого $\iota \in I$ (используя б), показать, что регулярное примитивное кольцо без нильпотент-

ных элементов является телом; см. упражнение 7 и § 5, упражнение 5д)).

г) Пусть (D_ι), $\iota \in I$,— бесконечное семейство тел, и $\mathfrak{F}$ — множество с возрастающей фильтрацией, состоящее из частей множества I и образующее покрытие I. Через B_H, $H \in \mathfrak{F}$, обозначим двусторонний идеал произведения $B = \prod_{\iota \in I} D_\iota$, являющийся произведением множеств D_ι для $\iota \in H$ и множеств $D'_\iota = \{0\} \subset D_\iota$ для $\iota \overline{\in} H$. Показать, что подкольцо A, порожденное в B единицей и объединением идеалов B_H, регулярно и не имеет нильпотентных элементов $\neq 0$.

18) Кольцо A называется *сильно n-регулярным* ($n > 0$ — целое число), если для любого $a \in A$ существует $x \in A$ такой, что $xa^{n+1} = a^n$.

а) Показать, что для всякого элемента $b \in \mathfrak{R}(A)$ $b^n = 0$ (заметить, что если $b^n = xb^{n+1}$, то $1 - xb$ обратим).

б) Показать, что сильно n-регулярное примитивное кольцо изоморфно кольцу матриц $\boldsymbol{M}_r(D)$ над телом, причем $r \leqslant n$ (заметить, что если подкольцо A плотно в кольце $\mathscr{L}(V)$ эндоморфизмов векторного пространства V размерности $> n$, то найдется такой элемент $b \in \mathscr{L}(V)$, что $b^n \neq 0$, $b^{n+1} = 0$).

в) Показать, что сильно n-регулярное кольцо является кольцом Цорна (упражнение 13). (Заметить прежде всего, что если $xa^{n+1} = a^n$, то $x^n a^{2n} = a^n$; используя б), упражнение 7а) § 6 и лемму 2 § 2, показать, что $a^n x a^n - a^n \in \mathfrak{R}(A)$. Наконец, с помощью упражнения 10а) показать, что если элементы y, z удовлетворяют условиям $y = zy^2$ и $yzy - y \in \mathfrak{R}(A)$, то существует элемент $t \in A$ такой, что $y = ty^2$ и $(ty)^2 = ty$.) Показать, что если кольцо A, кроме того, без радикала, то оно псевдорегулярно (упражнение 14).

г) Показать, что сильно n-регулярные кольца без нильпотентных элементов $\neq 0$ совпадают с регулярными кольцами без нильпотентных элементов $\neq 0$. (Заметив, что если e — идемпотент, лежащий в центре кольца A, и $ea^n = a^n$, то $(ea^{n-1} - a^{n-1})^2 = 0$, свести доказательство к случаю $n = 1$. С помощью а) и б) показать затем, что кольцо A изоморфно некоторому подкольцу произведения тел, и вывести отсюда, что если $a = xa^2$, то $xa = e$ является идемпотентом, лежащим в центре кольца A.)

д) Показать, что кольцо, определенное в упражнении 2, не является сильно n-регулярным ни для какого n.

*19) Пусть A — артиново кольцо и $l_A(A_s) = n$.

а) Показать, что A сильно n-регулярно (упражнение 18).

б) Показать, что A псевдорегулярно. (Пусть $(\mathfrak{R}(A))^r = \{0\}$ и $m = l_B(B_s)$, где $B = A/\mathfrak{R}(A)$; показать сначала, что для любого $b \in B$ существует элемент $y \in B$, перестановочный с b и такой, что $b^{m+1}y = b^m$; свести доказательство к случаю, когда B — простое кольцо, и применить лемму 2 § 2. Вывести отсюда, что для любого $a \in A$ существует $z \in A$ такой, что $a^{mr}za^{mr} = a^{mr}$.)

в) Пусть $\mathcal{J}$ — множество ненильпотентных левых идеалов кольца A. Показать, что всякий левый идеал кольца A является прямой суммой конечного числа идеалов Ae_i (e_i — идемпотенты) — минимальных элементов множества $\mathcal{J}$ — левого идеала, содержащегося в радикале (заметить, что ввиду а) всякий минимальный элемент I множества $\mathcal{J}$ содержит идемпотент $e \neq 0$ такой, что $I = Ie$).

г) Для того чтобы левый идеал n кольца A имел вид Ae, где $e \neq 0$ — идемпотент, необходимо и достаточно, чтобы n был прямой суммой конечного числа идеалов Ae_i — минимальных элементов множества $\mathcal{J}$, причем e_i составляли бы систему ортогональных идемпотентов (использовать в)).

20) Артиново кольцо A называется *примарным*, если $A/\mathfrak{R}(A)$ — простое кольцо, и *вполне примарным*, если $A/\mathfrak{R}(A)$ — тело.

Показать, что всякое примарное артиново кольцо изоморфно кольцу матриц $M_r(B)$ над вполне примарным кольцом (использовать упражнения 11 и 19г) § 6 и упражнение 9 § 1).

21) Пусть A — артиново кольцо, I — неразложимый ненильпотентный левый идеал, то есть (упражнение 19в)) минимальный элемент множества ненильпотентных левых идеалов; имеем $I = Ae$, где e — идемпотент $\neq 0$.

а) Показать, что всякий левый идеал, содержащийся в I и $\neq I$, содержится в $n = I \cap \mathfrak{R}(A)$; показать, что кольцо eAe, изоморфное кольцу эндоморфизмов A-модуля I (§ 1, упражнение 3б)), вполне примарно (упражнение 20) (см. § 2, предложение 4). Если $\bar{e}$ — канонический образ e в $\bar{A} = A/\mathfrak{R}(A)$, то фактормодуль I/n является простым A-модулем, изоморфным $\bar{A}\bar{e}$.

б) Для всякого A-модуля M eM является (eAe)-модулем. Если N — подмодуль в M, то $e(M/N)$ eAe-изоморфен $(eM)/(eN)$; кроме того, $(Ae)M$ — подмодуль в M и $e((Ae)M) = eM$. Вывести отсюда, что если A-модуль M прост, то либо $eM = \{0\}$, либо M изоморфен $\bar{A}\bar{e}$ и (eAe)-модуль eM прост.

*22) Пусть A — артиново кольцо, прямая сумма неразложимых левых идеалов Ae_i ($1 \leqslant i \leqslant n$), где e_i — ортогональные идемпотенты (упражнение 19г)).

а) Показать, что, в обозначениях упражнения 21а), длина (e_iAe_i)-модуля e_iAe_j равна числу факторов ряда Жордана — Гельдера A-модуля Ae_j, изоморфных $\bar{A}\bar{e}_i$ (применить упражнение 21б)).

б) Пусть R — отношение эквивалентности между модулями Ae_i, Ae_j: «существует такая последовательность индексов $(h_1, \ldots, h_m)$, что $h_1 = i$, $h_m = j$, и при $1 \leqslant s \leqslant m-1$ найдется фактор ряда Жордана — Гельдера модуля Ae_{h_s}, изоморфный фактору ряда Жордана — Гельдера модуля $Ae_{h_{s+1}}$». Классы эквивалентности левых идеалов по отношению R называются *блоками* левых идеалов. Пусть $\mathcal{B}_k$ ($1 \leqslant k \leqslant q$) — различные блоки, и a_k — сумма идеалов блока $\mathcal{B}_k$.

Показать, что идеалы a_k являются единственными неразложимыми двусторонними идеалами кольца A. (Чтобы убедиться, что a_k — двусторонний идеал, заметить с помощью а), что $Ae_ixe_j \subset Ae_j$ и при $e_iAe_j \neq \{0\}$ модули Ae_i и Ae_j сравнимы по mod R. С другой стороны, если ряды Жордана — Гельдера модулей Ae_i и Ae_j имеют общий фактор (с точностью до изоморфизма), то в силу упражнения 21 существует такой индекс h, что $e_hAe_r \neq \{0\}$ и $e_hAe_s \neq 0$. Заметив, что $e_hAe_r \subset (Ae_hA) \cap (Ae_rA)$ и $e_hAe_s \subset (Ae_hA) \cap (Ae_sA)$, вывести отсюда, что при любом разложении кольца A в прямую сумму двусторонних идеалов $\mathfrak{b}_t$, каждый из которых является прямой суммой некоторого числа Ae_i, идемпотенты e_r и e_s принадлежат одному и тому же идеалу $\mathfrak{b}_t$; применить предложение 6 гл. I, § 8, n° 10.)

в) Показать, что правые идеалы e_iA неразложимы (рассмотреть их канонические образы в $A/\mathfrak{R}(A)$).

г) Пусть A — алгебра конечного ранга над полем K; обозначим через c_{ij} (соответственно d_{ij}) число факторов ряда Жордана — Гельдера модуля $\overline{Ae_i}$ (соответственно $\overline{e_jA}$), изоморфных Ae_j (соответственно e_iA). Доказать равенство $c_{ij}r_j = d_{ji}r_i$, где r_i — ранг тела $(e_iAe_i)/(e_i\mathfrak{R}(A)\,e_i)$ над полем K (подсчитать размерность векторного пространства e_iAe_j над полем K и принять а)). Разобрать частный случай, когда поле K алгебраически замкнуто.

*23) а) Пусть A — артиново кольцо, все нильпотентные элементы которого лежат в центре. Показать, что A — прямая композиция конечного числа вполне примарных колец (рассматривая полупростое кольцо $A/\mathfrak{R}(A)$, показать, что, в обозначениях упражнения 22, $e_ix - xe_i \in \mathfrak{R}(A)$ при любом $x \in A$, и вывести отсюда, что идеал Ae_i двусторонний).

б) Предположим дополнительно, что A вполне примарно и $\mathfrak{R}(A) \neq \{0\}$. Показать, что $A/\mathfrak{R}(A)$ — поле (заметить, что при $x \in A$, $y \in A$, $z \in \mathfrak{R}(A)$ $(xy - yx)\,z = 0$).

*24) а) Показать, что в кольце $\boldsymbol{M}_n(D)$ матриц над телом D подкольцо T треугольных матриц (a_{ij}) таких, что $a_{ij} = 0$ при $i \leqslant j$, является максимальным нильпотентным подкольцом и всякое максимальное нильпотентное подкольцо имеет вид cTc^{-1}, где c — обратимый элемент в $\boldsymbol{M}_n(D)$ (см. § 2, упражнение 3).

б) Показать, что в артиновом кольце A пересечение максимальных нильпотентных подколец совпадает с радикалом и любые два таких подкольца переводятся друг в друга некоторым внутренним автоморфизмом (заметить, что всякое максимальное нильпотентное подкольцо содержит $\mathfrak{R}(A)$; заметив, что всякий элемент кольца A, класс которого по mod $\mathfrak{R}(A)$ обратим, сам обратим, применить а)).

25) Показать, что если кольцо A одновременно артиново слева и нетерово справа, то оно артиново справа (рассмотреть правые A-модули $(\mathfrak{R}(A))^k/(\mathfrak{R}(A))^{k+1}$ как $(A/\mathfrak{R}(A))$-модули).

*26) а) Пусть A — кольцо, S — мультипликативный подмоноид в A (подмножество, устойчивое относительно умножения); S называется *нильпотентным*, если существует целое число $m > 0$ такое, что $s_1 s_2 \dots s_m = 0$ для любой последовательности (s_i) из m элементов множества S. Предположим, что моноид S порождается конечным числом нильпотентных элементов кольца A, но не нильпотентен. Показать, что существуют элемент $b \in S$ и конечная последовательность элементов $c_i \in S$ такие, что мультипликативный моноид, порожденный элементами $a_i = bc_i$, не нильпотентен. (Среди образующих моноида S рассмотреть последовательность $(b_i)_{1 \leqslant i \leqslant m}$ такую, что моноид B_{m-1}, порожденный элементами $b_1, \dots, b_{m-1}$, нильпотентен, а моноид B_m, порожденный элементами $b_1, \dots, b_m$, не нильпотентен; заметить, что множество элементов вида $b_m^k c$, где $c \in B_{m-1}$, конечно.) Вывести отсюда, что существует целое число $h > 0$ такое, что $b^h S \neq \{0\}$, но $b^h a_i = 0$ для любого индекса i.

б) Пусть A — нетерово кольцо; показать, что всякий его левый нильидеал нильпотентен. (Заметить, что такой идеал имеет конечную систему образующих; рассмотреть мультипликативный моноид S, порожденный этими образующими, и применить упражнение а), используя левые аннуляторы мультипликативных подмоноидов моноида S.)

27) Пусть A — артиново кольцо, и пусть всякое кольцо B, содержащее A и имеющее ту же единицу, что и A, является свободным левым A-модулем. Показать, что кольцо A просто (см. § 5, n° 6, следствие предложения 13). (Для всякого двустороннего идеала $\mathfrak{a}$ кольца A, отличного от $\{0\}$ и от A, на произведении $A \times \mathfrak{a}$ определить структуру кольца — аналогично тому, как это было сделано в упражнении 4 § 2.)

28) Пусть M — A-модуль без радикала; показать, что кольцо гомотетий A_M без радикала (использовать лемму 4 § 2, n° 3).

29) Пусть A — кольцо и $A/\mathfrak{R}(A)$ полупросто. Показать, что $\mathfrak{R}(M) = \mathfrak{R}(A)\,M$ для любого A-модуля M (заметить, что $M/\mathfrak{R}(A)\,M$ является $(A/\mathfrak{R}(A))$-модулем).

30) а) Пусть A — кольцо без радикала и всякое множество его *моногенных* левых идеалов обладает минимальным элементом. Показать, что A полупросто (использовать упражнение 8 § 5 и упражнение 16 гл. I, § 8).

б) Пусть V — векторное пространство бесконечной размерности над телом D, A — подкольцо в кольце эндоморфизмов $\mathscr{L}_D(V)$, порожденное единицей и эндоморфизмами конечного ранга. Показать, что всякий левый идеал кольца A содержит некоторый минимальный идеал.

31) Пусть A — алгебра над полем K, $\mathfrak{a}$ — ее двусторонний идеал, и B — подалгебра, порожденная ее единицей и идеалом $\mathfrak{a}$. Показать, что радикал алгебры B содержится в радикале алгебры A (заметить,

что если M — простой A-модуль, то либо $ax = \{0\}$ для всех $x \in M$, либо $ax \in M$ для всех элементов $x \neq 0$ модуля M).

32) Пусть A — коммутативная полупростая алгебра конечного ранга над полем K, K_i $(1 \leqslant i \leqslant r)$ — ее простые компоненты, являющиеся расширениями конечной степени поля K. Пусть B — подалгебра в A, E_j $(1 \leqslant j \leqslant s)$ — ее простые компоненты. Показать, что в интервале $[1, r]$ множества N найдется s непустых подмножеств L_j, не имеющих попарно общих элементов и таких, что компонента E_j содержится в прямой композиции полей K_j для $i \in L_j$, $1 \leqslant j \leqslant s$. Отображение pr_i, суженное на E_j, при любом $i \in L_j$ будет изоморфизмом компоненты E_j на подполе E_{ji} в K_i. Доказать обратное утверждение. Вывести отсюда, что если все K_i сепарабельны над полем K, то алгебра A имеет лишь конечное число подалгебр (см. гл. V, § 10, n° 5, предложение 8).

33) а) Пусть A — артиново (слева) кольцо. Показать, что всякий правый идеал $\mathfrak{r} \subset A$ содержит некоторый минимальный правый идеал (рассмотреть пересечения $\mathfrak{r}$ со степенями радикала $\mathfrak{R}(A)$ и заметить, что правый идеал, аннулируемый справа радикалом $\mathfrak{R}(A)$, можно рассматривать как правый $A/\mathfrak{R}(A)$-модуль).

б) Показать, что левый (соответственно правый) цоколь артинова кольца A является правым (соответственно левым) аннулятором радикала $\mathfrak{R}(A)$. Вывести отсюда, что всякий минимальный двусторонний идеал кольца A содержится в пересечении правого и левого цоколей кольца A.

§ 7. Радикал и полупростота тензорных произведений

В этом параграфе K — поле; если A и B — алгебры над K, M — A-модуль, N — B-модуль, то через $M \otimes N$ часто обозначается тензорное произведение над полем K векторных пространств, полученных из M и N сужением кольца скаляров до K; алгебра $A \otimes_K B$ часто будет обозначаться через $A \otimes B$. Алгебры A и B будут отождествляться с подалгебрами в $A \otimes B$ посредством изоморфизмов $a \to a \otimes 1$ и $b \to 1 \otimes b$ (гл. III, § 3, n° 3).

1. *Предварительные замечания*

Пусть A, B — алгебры над полем K, C — алгебра $A \otimes B$, M — A-модуль, N — B-модуль. Отображение

$$(a, b, x, y) \to (ax) \otimes (by)$$

произведения $A \times B \times M \times N$ в $M \otimes N$ K-полилинейно; поэтому (гл. III, § 1, n° 2) существует единственное билинейное ото-

бражение $(c, z) \to cz$ произведения $C \times (M \otimes N)$ в $M \otimes N$ такое, что

$$(a \otimes b)(x \otimes y) = (ax) \otimes (by); \qquad (1)$$

легко проверить, что это отображение определяет на $M \otimes N$ структуру *C-модуля*; рассматривая $M \otimes N$ как C-модуль, мы всегда будем подразумевать, что речь идет о только что определенной структуре.

В частности, если M — A-модуль A_s, то $A \otimes N$ канонически наделяется структурой C-модуля; впрочем, $A \otimes N$ канонически отождествляется с $A \otimes_K (B \otimes_B N)$, то есть с $(A \otimes_K B) \otimes_B N = C \otimes_B N$ (гл. III, приложение II, n°n° 4 и 9); более того, если a, $a' \in A$, $b \in B$, $c \in N$, то $a' \otimes y$ отождествляется с $(a' \otimes 1) \otimes y$, а $(a \otimes b)(a' \otimes y) = (aa') \otimes (by)$ с $(aa' \otimes b) \otimes y$. Таким образом, C-модуль $A \otimes N$ отождествляется с C-модулем $C \otimes_B N$, получающимся из N расширением кольца скаляров до C (гл. III, приложение II, n° 10).

Отображение $y \to 1 \otimes y$ модуля N в $A \otimes N$ инъективно, так как A и N — векторные пространства над K (гл. III, § 2, n° 2, теорема 1); тензорное произведение $A \otimes N$ наделяется структурой B-модуля, получаемой сужением до B кольца скаляров C, и указанное отображение является гомоморфизмом B-модулей: если $b \in B$, $y \in N$, то $(1 \otimes b)(1 \otimes y) = 1 \otimes (by)$. Отождествим N с его образом в $A \otimes N$ при отображении $1 \to 1 \otimes y$. Тогда всякое векторное подпространство N' в N (над полем K) отождествляется с некоторым векторным подпространством в $A \otimes N$; с другой стороны, тензорное произведение $A \otimes N'$ $(= A \otimes_K N')$ отождествляется с некоторым подпространством в $A \otimes N$ (гл. III, § 1, n° 3, следствие 3 предложения 7); после этих отождествлений выполняется равенство

$$(A \otimes N') \cap N = N'. \qquad (2)$$

В этом легко убедиться, разложив N в прямую сумму N' и его дополнительного подпространства (гл. III, n° 3, следствие 1 предложения 7).

Заметим, что при $N = B_s$ только что рассмотренная структура C-модуля на $C = A \otimes B$ представляет собой не что иное, как структуру C-модуля C_s.

2. *Расширение скаляров и радикал*

Предложение 1. Пусть A, B — алгебры над полем K, $C = A \otimes B$, N — B-модуль. Тогда

$$N \cap \mathfrak{R}_C(A \otimes N) \subset \mathfrak{R}_B(N). \tag{3}$$

Благодаря отождествлениям, сделанным в n° 1, этот результат является частным случаем следующей леммы:

Лемма 1. *Пусть B, C — кольца такие, что B — подкольцо в C, содержащее его единицу, и C — свободный правый B-модуль; пусть f — каноническое отображение $y \to 1 \otimes y$ B-модуля N в тензорное произведение $C \otimes_B N$, рассматриваемое как левый C-модуль. Тогда*

$$f^{-1}(\mathfrak{R}_C(C \otimes_B N)) \subset \mathfrak{R}_B(N). \tag{4}$$

Покажем сначала, что если модуль N прост, то левая часть (4) сводится к 0. В самом деле, пусть $y \neq 0$ — элемент N; так как он порождает B-модуль N, то $f(y)$ порождает C-модуль $C \otimes_B N$. Но модуль $C \otimes_B N$ не сводится к 0, так как правый B-модуль C свободен (гл. III, приложение II, n° 6, следствие предложения 5); следовательно (§ 6, n° 2, предложение 1), элемент $f(y)$ не содержится в радикале модуля $C \otimes_B N$, что доказывает наше утверждение. Предположим теперь, что N — произвольный B-модуль и элемент $y \in N$ таков, что $1 \otimes y \in \mathfrak{R}_C(C \otimes_B N)$; если u — B-гомоморфизм модуля N в простой B-модуль P, то $1 \otimes u$ — C-гомоморфизм модуля $C \otimes_B N$ в $C \otimes_B P$ и, следовательно (§ 6, n° 2, предложение 2), элемент $1 \otimes u(y) = (1 \otimes u)(1 \otimes y)$ входит в радикал модуля $C \otimes_B P$, то есть, по предыдущему, $u(y) = 0$. Тогда, по определению, $y \in \mathfrak{R}_B(N)$.

Предложение 1 не позволяет утверждать ни того, что из равенства $\mathfrak{R}_B(N) = 0$ следует $\mathfrak{R}_C(A \otimes N) = 0$, ни того, что из $\mathfrak{R}_C(A \otimes N) = 0$ следует $\mathfrak{R}_B(N) = 0$. Эти утверждения, вообще говоря, неверны (см. n° 3, теорема 1 и упражнения 4 и 5). Как мы сейчас увидим, они остаются верными в некоторых частных случаях.

Предложение 2. *Пусть A, B — алгебры над полем K, $C = A \otimes B$, N — B-модуль. Равенство*

$$N \cap \mathfrak{R}_C(A \otimes N) = \mathfrak{R}_B(N) \qquad (5)$$

выполняется в каждом из следующих трех случаев:

а) *размерность алгебры A над K конечна*;

б) *N — B-модуль конечного типа, и A — объединение семейства с возрастающей фильтрацией подалгебр конечной размерности над полем K* (это выполняется, например, когда A — поле, *алгебраическое* расширение поля K);

в) *$N = B_s$, и радикал алгебры B нильпотентен* (это выполняется, например, когда A — *артиново* кольцо (§ 6, n° 4, теорема 3)).

Вследствие (3) достаточно доказать включение $\mathfrak{R}_B(N) \subset \subset \mathfrak{R}_C(A \otimes N)$.

а) Пусть алгебра A конечномерна над K, и v — C-гомоморфизм модуля $A \otimes N$ в простой C-модуль P; достаточно доказать, что v аннулируется на $\mathfrak{R}_B(N)$. Однако сужение гомоморфизма v на N будет B-гомоморфизмом модуля N в P, рассматриваемым как B-модуль, и справедливо включение $v(\mathfrak{R}_B(N)) \subset \subset \mathfrak{R}_B(P)$ (§ 6, n° 2, предложение 2); достаточно поэтому показать, что $\mathfrak{R}_B(P) = \{0\}$. В алгебре C всякий элемент из A перестановочен со всеми элементами из B, так что гомотетии C-модуля P, определяемые элементами из A, являются эндоморфизмами B-модуля P; следовательно (§ 6, n° 2, предложение 2), радикал $\mathfrak{R}_B(P)$ будет в P одновременно B-подмодулем и A-подмодулем, то есть и C-подмодулем; так как P — простой C-модуль, то $\mathfrak{R}_B(P)$ равен либо $\{0\}$, либо P. Однако C-модуль прост (то есть моногенен), а алгебра A конечномерна над K, и поэтому B-модуль P конечного типа, и следовательно, $\mathfrak{R}_B(P) \neq P$ (§ 6, n° 2, предложение 1); это показывает, что $\mathfrak{R}_B(P) = \{0\}$.

б) Пусть модуль N порождается конечным числом элементов x_j $(1 \leqslant j \leqslant n)$, и A — объединение возрастающего фильтрующего семейства $(A_\iota)_{\iota \in I}$ подалгебр конечной размерности над полем K. Пусть $x \in \mathfrak{R}_B(N)$; докажем, что $x \in \mathfrak{R}_C(A \otimes N)$. Так как элементы x_j образуют систему образующих C-модуля $A \otimes N$, то достаточно показать (§ 6, n° 2, предложение 4), что при любых $c_j \in C$ $(1 \leqslant j \leqslant n)$ элементы $x_j + c_j x$ также порождают C-модуль

$A \otimes N$. Однако найдется индекс $\iota \in I$ такой, что все элементы c_j входят в $C_\iota = A_\iota \otimes B$. Из а) следует, что $x \in \mathfrak{R}_{C_\iota}(A_\iota \otimes N)$, и следовательно, элементы $x_j + c_j x$ порождают C_ι-модуль $A_\iota \otimes N$; отсюда вытекает, что C-модуль, порожденный в $A \otimes N$ этими элементами, содержит N, то есть равен $A \otimes N$, что и заканчивает доказательство в рассматриваемом случае.

в) Предположим, наконец, что $(\mathfrak{R}(B))^k = \{0\}$. Так как всякий элемент из A перестановочен со всеми элементами из B, то двусторонний идеал J, порожденный в C радикалом $\mathfrak{R}(B)$, состоит из конечных сумм $\sum_i a_i r_i$, где $a_i \in A$, $r_i \in \mathfrak{R}(B)$. Следовательно, $J^k = \{0\}$, так что J содержится в радикале кольца C (§ 6, п° 3, следствие 3 теоремы 1). Тем более справедливо включение $\mathfrak{R}(B) \subset \mathfrak{R}(C)$; это заканчивает доказательство предложения 2.

Следствие. *Пусть A, B — алгебры над полем K. Если B — артиново кольцо и алгебра $A \otimes B$ без радикала, то B полупросто.*

В самом деле, из предложения 2 следует, что кольцо B без радикала, то есть полупросто (§ 6, п° 4, следствие 2 теоремы 4).

Предложение 3. *Пусть B — алгебра над полем K, A — тело, содержащее K в своем центре, $C = A \otimes B$, N — B-модуль. Равенство*

$$\mathfrak{R}_C(A \otimes N) = A \otimes (N \cap \mathfrak{R}_C(A \otimes N)) \tag{6}$$

выполняется в каждом из следующих случаев:

а) *K — поле инвариантных элементов некоторой группы автоморфизмов тела A* (это выполняется, если *K — центр* тела A или A коммутативно и является расширением Галуа поля K);

б) *N — B-модуль конечного типа, и A — поле, сепарабельное расширение* (алгебраическое или трансцендентное) *поля K.*

Предположим сначала, что выполнено условие а). Достаточно показать, что радикал $\mathfrak{R}_C(A \otimes N)$ имеет вид $A \otimes N'$, где N' — векторное подпространство векторного K-пространства N; в самом деле, тогда по формуле (2) $N' = N \cap \mathfrak{R}_C(A \otimes N)$. Пусть u — автоморфизм тела A, оставляющий инвариантными элементы поля K; из формулы (1) следует, что автоморфизм $u \otimes 1$ векторного K-пространства $A \otimes N$ переставляет между собой C-подмодули в $A \otimes N$; этот автоморфизм переставляет

также между собой максимальные подмодули C-модуля $A \otimes N$ и, следовательно, оставляет инвариантным пересечение этих подмодулей, то есть радикал $\mathfrak{R}_C(A \otimes N)$. Поэтому доказываемое утверждение вытекает из предложения 7 § 4, n° 5.

Теперь рассмотрим условие б); пусть $N' = N \cap \mathfrak{R}_C(A \otimes N)$; достаточно показать, что $\mathfrak{R}_C(A \otimes N) \subset A \otimes N'$. Пусть $z = \sum_{i=1}^{m} a_i \otimes y_i$ ($a_i \in A$, $y_i \in N$)— элемент радикала $\mathfrak{R}_C(A \otimes N)$; можно предполагать, что элементы a_i линейно независимы над полем K, и тогда остается показать, что $y_i \in \mathfrak{R}_C(A \otimes N)$ при любом i (откуда будет следовать, что $y_i \in N'$). Пусть Ω — алгебраическое замыкание поля A, и u — K-автоморфизм поля Ω; $u \otimes 1$ можно рассматривать как изоморфизм модуля $A \otimes N$ на $(u(A) \otimes B)$-модуль $u(A) \otimes N$; следовательно, элемент $(u \otimes 1)(z) = \sum_{i=1}^{m} u(a_i) \otimes y_i$ принадлежит радикалу модуля $u(A) \otimes N$. Однако алгебра $\Omega \otimes B$ над полем K канонически отождествляется с $\Omega \otimes_{u(A)} (u(A) \otimes B)$, а $(\Omega \otimes B)$-модуль $\Omega \otimes N$ — с $\Omega \otimes_{u(A)} (u(A) \otimes N)$ (гл. III, приложение II, n°n° 4 и 9); так как Ω — алгебраическое расширение поля $u(A)$, то ввиду предложения 2б) элемент $(u \otimes 1)(z)$ принадлежит радикалу модуля $\Omega \otimes N$. Поскольку поле A сепарабельно над K, существуют такие K-автоморфизмы u_i поля Ω ($1 \leqslant i \leqslant m$), что матрица $(u_i(a_j))$ с элементами из поля Ω обратима (гл. V, § 7, n° 2); пусть (μ_{ij}) — обратная к ней матрица. Тогда $\sum_{j=1}^{m} \mu_{ij}(u_j \otimes 1)(z) = \sum_{j,k} \mu_{ij}(u_j(a_k) \otimes y_k) = 1 \otimes y_i$ принадлежит радикалу модуля. Но мы видели выше, что $(\Omega \otimes B)$-модуль $\Omega \otimes N$ отождествляется с модулем $\Omega \otimes_A (A \otimes N)$ над $\Omega \otimes_A (A \otimes B) = \Omega \otimes_A C$; тогда по формуле (3) $y_i \in \mathfrak{R}_C(A \otimes N)$ при всех i, что и заканчивает доказательство.

Следствие 1. *При условиях* а) *или* б) *предложения* 3 *имеет место включение*

$$\mathfrak{R}_C(A \otimes N) \subset A \otimes \mathfrak{R}_B(N). \tag{7}$$

В самом деле, это вытекает из предложения 3 и формулы (3) (см. n° 6, следствие 1 теоремы 3).

Следствие 2. *Пусть B — алгебра над полем K, N — B-модуль, A — поле, сепарабельное расширение поля K. Тогда*

$$\mathfrak{R}_{A\otimes B}(A\otimes N) = A\otimes \mathfrak{R}_B(N) \tag{8}$$

в каждом из следующих случаев:

а) *A имеет конечную степень над K;*

б) *A алгебраично над K, и N — B-модуль конечного типа;*

в) *$N = B_s$, и радикал алгебры B нильпотентен.*

Утверждения б) и в) немедленно следуют из формул (5) и (6). Если A — *расширение Галуа* поля K, то а) также следует из этих формул (предложение 3а)). Если A — сепарабельное расширение конечной степени над полем K, то нормальное расширение E поля K, порожденное полем A в алгебраическом замыкании поля A, будет расширением Галуа конечной степени поля K (гл. V, § 6, n° 3, следствие 1 предложения 9 и § 10, n° 3, предложение 6). Следовательно, $\mathfrak{R}_{E\otimes B}(E\otimes N) = E\otimes \mathfrak{R}_B(N)$. С другой стороны, алгебра $E\otimes B$ (соответственно $(E\otimes B)$-модуль $E\otimes N$) канонически отождествляется с алгеброй $E\otimes_A(A\otimes B)$ (соответственно с модулем $E\otimes_A(A\otimes N)$ над этой алгеброй) (гл. III, приложение II, n°n° 4 и 9). Так как поле E конечного ранга над A, то по предложению 2а) $(A\otimes N)\cap \mathfrak{R}_{E\otimes B}(E\otimes N) = \mathfrak{R}_{A\otimes B}(A\otimes N)$, то есть $\mathfrak{R}_{A\otimes B}(A\otimes N) = (A\otimes N)\cap(E\otimes \mathfrak{R}_B(N))$; но это пересечение равно $A\otimes \mathfrak{R}_B(N)$, в чем можно убедиться, взяв в E (соответственно в N) базис над полем K, содержащий базис поля A (соответственно $\mathfrak{R}_B(N)$) (гл. III, § 1, n° 3, следствие 2 предложения 7).

3. Тензорное произведение полей

Предложение 4. *Пусть E, F — поля, расширения поля K. Радикал алгебры $E\otimes F$ совпадает с множеством ее нильпотентных элементов.*

Пусть Ω — алгебраическое замыкание поля E; применив предложение 2а) к случаю $K = E$, $A = \Omega$, $N = (E\otimes F)_s$, получим, что радикал алгебры $E\otimes F$ содержится в радикале алгебры $\Omega\otimes F$, отождествленной с $\Omega\otimes_E(E\otimes F)$. Пусть p — характеристическая экспонента поля K, $R = K^{p^{-\infty}}$ — поле инвариантных элементов группы K-автоморфизмов поля Ω (гл. V, § 8, n° 1).

Применив следствие 1 предложения 3 (n° 2) к случаю $A = \Omega$, $K = R$, $N = (R \otimes F)_s$ (алгебра $\Omega \otimes F$ отождествлена с $\Omega \otimes_R (R \otimes F)$), получим, что радикал алгебры $\Omega \otimes F$ содержится в идеале, порожденном радикалом алгебры $R \otimes F$; предположим, что все элементы последнего радикала нильпотентны; тогда нильпотентны и все элементы радикала алгебры $\Omega \otimes F$, а следовательно, и радикала алгебры $E \otimes F$; так как, обратно, всякий нильпотентный элемент алгебры $E \otimes F$ содержится в радикале (§ 6, n° 3, следствие 3 теоремы 1), то предложение 4 будет доказано, если мы установим справедливость нашего предположения. Пусть $z = \sum_i x_i \otimes y_i \in \mathfrak{R}(R \otimes F)$ $(x_i \in R, \quad y_i \in F)$. Существует такое целое число $m \geqslant 0$, что для любого индекса i $x_i^{p^m} \in K$, откуда $z^{p^m} = \sum_i x_i^{p^m} \otimes y_i^{p^m} = 1 \otimes \left(\sum_i x_i^{p^m} y_i^{p^m}\right)$. Следовательно, z^{p^m} принадлежит подполю F в $R \otimes F$; но этот элемент принадлежит радикалу и, следовательно, не может быть обратимым; поэтому $z^{p^m} = 0$

Теорема 1. *Пусть p — характеристическая экспонента поля K, E — расширение поля K. Следующие условия эквивалентны:*

а) *E — сепарабельное расширение поля K;*

б) *алгебра $E \otimes F$ является алгеброй без радикала для любого расширения F поля K;*

в) *алгебра $E \otimes F$ не имеет ненулевых нильпотентных элементов при любом расширении F поля K;*

г) *$E \otimes K^{p^{-1}}$ не имеет ненулевых нильпотентных элементов.*

Следствие 1 предложения 3 показывает, что а) влечет б); условия б) и в) эквивалентны по предложению 4; кроме того, в) тривиально влечет б). Чтобы убедиться, наконец, что из г) следует а), предположим, что расширение E не сепарабельно над K; тогда по критерию Маклейна (гл. V, § 8, n° 2, предложение 3) существуют элементы $x_i \in E$, линейно независимые над полем K $(1 \leqslant i \leqslant n)$, и отличные от нуля элементы $a_i \in K^{p^{-1}}$ такие, что $\sum_{i=1}^{n} a_i x_i = 0$ в алгебраическом замыкании поля E. Следовательно, $\sum_{i=1}^{n} a_i^p x_i^p = 0$, и поскольку $a_i^p \in K$, то $\left(\sum_{i=1}^{n} x_i \otimes a_i\right)^p = \left(\sum_{i=1}^{n} x_i^p a_i^p\right) \otimes 1$ в алгебре

$E \otimes K^{p^{-1}}$; однако в этой алгебре $\sum_{i=1}^{n} x_i \otimes a_i = 0$, и таким образом, из г) следует а).

Следствие 1. *Пусть E_i $(1 \leqslant i \leqslant n)$ — расширения поля K, сепарабельные все, кроме, быть может, одного, и не более чем одно из них не имеет конечной степени над K. Тогда тензорное произведение $E_1 \otimes E_2 \otimes \ldots \otimes E_n$ является прямым произведением полей.*

Проведем индукцию по n. При $n = 1$ доказывать нечего; если $n = 2$, то по теореме 1 радикал алгебры $E_1 \otimes E_2$ равен нулю; более того, если, например, E_2 конечного ранга над K, то $E_1 \otimes E_2$ конечного ранга над E_1, то есть является коммутативным артиновым кольцом без радикала и, следовательно, прямой композицией полей (§ 6, n° 4, предложение 9). Если $n > 2$, то можно предполагать, что расширения E_i, $i > 2$, сепарабельны и имеют конечную степень над K; тогда, по предположению индукции, $E_1 \otimes E_2 \otimes \ldots \otimes E_{n-1}$ является прямой композицией полей, и доказательство сводится к случаю двух расширений.

Следствие 2. *Пусть E — расширение поля K, f — неприводимый многочлен из кольца $K[X]$, F — поле $K[X]/(f)$. Если одно из полей E и F сепарабельно над K, то f разлагается в $E[X]$ в произведение $f_1 f_2 \ldots f_r$ различных неприводимых многочленов и алгебра $E \otimes F$ изоморфна прямой композиции полей $E[X]/(f_i)$ $(1 \leqslant i \leqslant r)$.*

В самом деле, алгебра $E \otimes F$ изоморфна $E[X]/(f)$ (гл. III, § 1, n° 3, предложение 6), и из теоремы 1 следует, что она без радикала; тогда следствие вытекает из предложения 8 § 6.

Если поле F сепарабельно над K, то следствие легко доказывается и без использования теоремы 1, устанавливая еще раз, что алгебра $E \otimes F$ без радикала: достаточно заметить, что многочлен f, имеющий лишь простые корни в алгебраическом замыкании поля K (гл. V, § 7, n° 6, предложение 9), является в $E[X]$ произведением различных неприводимых многочленов.

4. Тензорное произведение полупростых модулей

Теорема 2. *Пусть A, B — алгебры над полем K, M — A-модуль, N — B-модуль, C — алгебра $A \otimes B$.*

а) *Если $M \otimes N$ — полупростой* (соответственно *простой*) *C-модуль и $M \neq \{0\}$, $N \neq \{0\}$, то модули M и N полупросты* (соответственно *просты*).

б) *Пусть M и N просты; пусть E и F — тела, коммутанты модулей M и N соответственно, S и T — центры E и F соответственно. Для того чтобы C-модуль $M \otimes N$ был без радикала* (соответственно *прост, полупрост*), *необходимо и достаточно, чтобы алгебра $S \otimes T$ была без радикала* (соответственно $E \otimes F$ *было телом, полупростым кольцом*).

а) Пусть модуль $M \otimes N$ полупрост, и N' — подмодуль в N. Тогда $M \otimes N'$ является C-подмодулем в $M \otimes N$, и следовательно, существует C-линейное проектирование e модуля $M \otimes N$ на $M \otimes N'$. Так как $M \neq \{0\}$, то существуют элемент $x \in M$ и K-линейная форма h на векторном пространстве M такие, что $h(x) = 1$. B-гомоморфизм $y \to (h \otimes 1)(e(x \otimes y))$ модуля N в $K \otimes N'$ каждый элемент $z \in N'$ переводит в $1 \otimes z \in K \otimes N'$. Отождествляя канонически $K \otimes N'$ и N', получим проектирование модуля N на N'; это доказывает, что модуль N полупрост. Если модуль N не прост, то он разлагается в прямую сумму двух ненулевых подмодулей N' и N''; тогда подмодули $M \otimes N'$ и $M \otimes N''$ в $M \otimes N$ не равны нулю (гл. III, § 1, n° 3, следствие 1 предложения 7), и $M \otimes N$ является прямой суммой этих подмодулей; это показывает, что модуль $M \otimes N$ не прост.

б) Рассмотрим сначала *произвольные* A-модуль M и B-модуль N; пусть E — коммутант M, F — коммутант N. B-модуль N канонически отождествляется с $F_d \otimes_F N$ (гл. III, приложение II, n° 4); тогда векторное K-пространство $M \otimes N$ канонически отождествляется с $M \otimes (F_d \otimes_F N)$, а следовательно, и с $(M \otimes F_d) \otimes_F N$ (гл. III, приложение II, n° 9); определенный таким образом канонический изоморфизм φ векторного K-пространства $(M \otimes F_d) \otimes N$ на векторное K-пространство $M \otimes N$ обозначим через φ. Напомним еще, что через F_r обозначается множество F_d, рассматриваемое как левый модуль над кольцом F^0, противоположным F (§ 1, n° 2); произведение $M \otimes F_r$ канонически наделяется структурой $(A \otimes F^0)$-модуля (n° 1) и как векторное K-пространство совпадает, очевидно, с $M \otimes F_d$.

Теперь докажем лемму:

Лемма 2. *Пусть N — простой B-модуль, и M — A-модуль. Отображение $P \to \varphi(P \otimes_F N)$ является изоморфизмом (для структуры порядка по включению) упорядоченного множества*

$(A \otimes F^0)$-подмодулей модуля $M \otimes F_r$ на упорядоченное множество C-подмодулей модуля $M \otimes N$ и переводит радикал модуля $M \otimes F_r$ в радикал модуля $M \otimes N$.

Заметим, что C-подмодули в $M \otimes N$ — это в точности B-подмодули модуля $M \otimes N$, *устойчивые* относительно гомотетий, определяемых элементами алгебры A; аналогично $(A \otimes F^0)$-подмодули в $M \otimes F_r$ — это в точности векторные подпространства правого векторного F-пространства $M \otimes F_d$, *устойчивые* относительно гомотетий, определяемых элементами алгебры A; тогда первое утверждение леммы немедленно следует из предложения 6 § 4, n° 5. В частности, биекция $P \to \varphi(P \otimes_F N)$ ставит во взаимно однозначное соответствие максимальные подмодули в $M \otimes F_r$ и максимальные подмодули в $M \otimes N$; поскольку радикал модуля является наибольшим идеалом, содержащимся во всех максимальных подмодулях, то это отображение переводит радикал $M \otimes F_r$ в радикал $M \otimes N$.

Заметим теперь, что тензорное произведение $M \otimes N$ канонически наделено структурой $(E \otimes F)$-модуля (n° 1); гомотетии этого $(E \otimes F)$-модуля коммутируют с гомотетиями C-модуля $M \otimes N$, так что тензорное произведение $(E \otimes F)_d \otimes_{(E \otimes F)} (M \otimes N)$ можно отождествить с C-модулем $M \otimes N$ (гл. III, приложение II, n° 4); через $\mathfrak{r}(M \otimes N)$, где $\mathfrak{r}$ — произвольный правый идеал в $E \otimes F$, обозначим канонический образ тензорного произведения $\mathfrak{r} \otimes_{(E \otimes F)} (M \otimes N)$ в $M \otimes N$.

Лемма 3. *Пусть M — простой A-модуль, N — простой B-модуль. Отображение $\mathfrak{r} \to \mathfrak{r}(M \otimes N)$ является изоморфизмом (для структуры порядка по включению) упорядоченного множества правых идеалов в $E \otimes F$ на упорядоченное множество C-подмодулей в $M \otimes N$ и переводит радикал алгебры $E \otimes F$ в радикал модуля $M \otimes N$.*

Так как алгебры $E \otimes F$ и $F \otimes E$ канонически изоморфны, то правые идеалы в $E \otimes F$ можно отождествить с $(F^0 \otimes E^0)$-подмодулями в $F_r \otimes E_r$; с другой стороны, как и выше, можно определить канонический изоморфизм ψ тензорного произведения $(F_r \otimes E_r) \otimes_E M$ на $M \otimes F_r$ (для структуры векторных K-пространств); в качестве ψ взять композицию канонических изоморфизмов $F_r \otimes M$ на $M \otimes F_r$, $F_r \otimes (E_d \otimes_E M)$ на $F_r \otimes M$ и $(F_r \otimes E_r) \otimes_E M$ на $F_r \otimes (E_d \otimes_E M)$. Применяя лемму 2

с $A = F^0$, $M = F_r$, $B = A$, $N = M$, получим, что отображение $\mathfrak{r} \to \psi(\mathfrak{r} \otimes_E M)$ является изоморфизмом упорядоченного множества правых идеалов алгебры $E \otimes F$ на упорядоченное множество $(A \otimes F^0)$-подмодулей модуля $M \otimes F_r$ и переводит радикал алгебры $E \otimes F$ в радикал модуля $M \otimes F_r$. Тогда лемма 3 следует из леммы 2 и того факта, что, как легко вывести из формулы (1), подмодуль $\mathfrak{r} \cdot (M \otimes N)$ модуля $M \otimes N$ может быть записан в виде $\varphi(\psi(\mathfrak{r} \otimes_E M) \otimes_F N)$.

Из леммы 3 следует уже, что модуль $M \otimes N$ прост тогда и только тогда, когда $E \otimes F$ — тело (гл. I, § 9, n° 3, предложение 3), и полупрост тогда и только тогда, когда алгебра $E \otimes F$ полупроста; для доказательства второго утверждения, по определению полупростого кольца (§ 5, n° 1), достаточно заметить, что изоморфизм $\mathfrak{r} \to \mathfrak{r}(M \otimes N)$ упорядоченных множеств, установленный в лемме 3, ставит в соответствие друг другу прямые слагаемые модулей $(E \otimes F)_d$ и $M \otimes N$ (в самом деле, для того чтобы некоторый модуль X был прямой суммой подмодулей Y, Z, необходимо и достаточно, чтобы X и $\{0\}$ были соответственно верхней и нижней границами подмодулей Y и Z в упорядоченном множестве подмодулей модуля X). С другой стороны, лемма 3 показывает, что условия $\mathfrak{R}_C(M \otimes N) = 0$ и $\mathfrak{R}(E \otimes F) = 0$ равносильны. Но алгебру $E \otimes F$ можно отождествить с $E \otimes_S (F \otimes_T (S \otimes T))$ (гл. III, приложение II, n°n° 4 и 9); дважды применяя следствие 1 предложения 3 (условие а) предложения 3 выполнено), получим, что радикал $\mathfrak{R}(E \otimes F)$ содержится в двустороннем идеале $(E \otimes F) \cdot \mathfrak{R}(S \otimes T)$, порожденном радикалом $\mathfrak{R}(S \otimes T)$. Обратно, элементы радикала $\mathfrak{R}(S \otimes T)$ нильпотентны (n° 3, предложение 4) и принадлежат центру алгебры $E \otimes F$, то есть радикалу этой алгебры (§ 6, n° 3, замечания после следствия 3 теоремы 1); поэтому $\mathfrak{R}(E \otimes F) = (E \otimes F) \cdot \mathfrak{R}(S \otimes T)$; в частности, равенство $\mathfrak{R}(E \otimes F) = 0$ равносильно $\mathfrak{R}(S \otimes T) = 0$, что и заканчивает доказательство теоремы 2.

Следствие 1. *Пусть M и N — изотипные полупростые модули, один из которых имеет конечную размерность над K. Если центр кольца $F = \mathscr{L}_B(N)$ равен K, то $M \otimes N$ — изотипный полупростой C-модуль.*

Пусть N — изотипный модуль типа P; если тело D — коммутант модуля P, то, как известно, кольцо $\mathscr{L}_B(N)$ изоморфно $\mathscr{L}_D(V)$, где V — правое векторное пространство над телом D (§ 4, n° 4, предложение 4), и его центр, следовательно, отождествляется с центром тела D (§ 1, n° 3, предложение 6). Из предположений следствия вытекает, таким образом, что центр тела $D = \mathscr{L}_B(P)$ равен K.

Тогда можно ограничиться случаем, когда модули M и N простые. В обозначениях теоремы 2 имеем равенство $S \otimes T = S \otimes K$. Алгебра $S \otimes K$ является полем, изоморфным S, и модуль $M \otimes N$, следовательно, без радикала. Кроме того, если модуль M (соответственно N) имеет конечную размерность над полем K, то $M \otimes N$ является B-модулем (соответственно A-модулем) конечной длины и *тем более* C-модулем конечной длины; будучи без радикала, модуль $M \otimes N$ является полупростым C-модулем (§ 6, n° 4, теорема 4). По теореме 2 $E \otimes F$ — полупростое кольцо; легко видеть, что в обозначениях леммы 3 модули $\mathfrak{r} \cdot (M \otimes N) = \varphi(\psi(\mathfrak{r} \otimes {}_E M) \otimes {}_F N)$ и $\mathfrak{r}' \cdot (M \otimes N) = \varphi(\psi(\mathfrak{r}' \otimes_E M) \otimes_F N)$, где $\mathfrak{r}$ и $\mathfrak{r}'$ — минимальные правые идеалы в $E \otimes F$, изоморфные как правые $(E \otimes F)$-модули, являются изоморфными простыми C-модулями; ввиду леммы 3 остается доказать, что $(E \otimes F)_d$ является изотипным правым $(E \otimes F)$-модулем, или, что то же самое, алгебра $E \otimes F$ *проста* (§ 5, n° 2, предложение 8 и n° 4, следствие 3 теоремы 2). Пусть, однако, $\mathfrak{a} \neq \{0\}$ — двусторонний идеал алгебры $E \otimes_K F$; $\mathfrak{a}$ является векторным подпространством правого векторного F-пространства $E \otimes_K F$, устойчивым относительно отображений $1 \otimes f$, где f пробегает множество внутренних автоморфизмов тела F. Так как K есть центр F, то из предложения 7 § 4, n° 5, вытекает, что $\mathfrak{a} = V \otimes_K F$, где V — векторное подпространство в E (над полем K); следовательно (формула (2)), $V = \mathfrak{a} \cap E$; ясно, что V является идеалом тела E и не сводится к 0, так как $\mathfrak{a} \neq \{0\}$. Поэтому $V = E$ и $\mathfrak{a} = E \otimes F$, что и заканчивает доказательство.

Следствие 2. *Пусть A, B — простые алгебры над полем K, одна из которых конечного ранга над K, и центр одной из них равен K. Тогда алгебра $A \otimes B$ проста.*

Учитывая следствие предложения 8 § 5, n° 2, достаточно применить следствие 1 в случае $M = A_s$ и $N = B_s$.

Следствие 3. *Пусть A — центральная простая алгебра конечного ранга m над полем K и Ω — алгебраическое замыкание поля K; алгебра $A_{(\Omega)}$ изоморфна некоторой алгебре матриц $\boldsymbol{M}_r(\Omega)$ над полем Ω, и $m = r^2$.*

В самом деле, по следствию 2 алгебра $A_{(\Omega)} = A \otimes \Omega$ (как алгебра над полем Ω) проста и имеет конечный ранг над Ω; кроме того, ее центр равен Ω (§ 1, n° 2, следствие предложения 3). Поэтому утверждение вытекает из следствия 3 к предложению 12 § 5, n° 4, и того факта, что $A_{(\Omega)}$ имеет над полем Ω ранг m.

5. Сепарабельные модули и алгебры

Определение 1. *Пусть A — алгебра над полем K. A-модуль M называется сепарабельным (над K), если для любого расширения E поля K $(E \otimes A)$-модуль $E \otimes M$ является модулем без радикала. Алгебра A называется сепарабельной (над K), если для любого расширения E поля K алгебра $E \otimes A$ без радикала.*

Утверждение, что A — сепарабельная алгебра, равносильно, таким образом, тому, что модуль A_s сепарабелен над K; теорема 1 показывает, что если A — поле, то определенное здесь свойство сепарабельности совпадает с понятием сепарабельности расширения, определенным в гл. V, § 7, n° 2.

Всякий подмодуль сепарабельного над K модуля сепарабелен над K (см. § 6, n° 2, предложение 3); всякая прямая сумма модулей, сепарабельных над K, сепарабельна над K (см. § 6, n° 2, следствие 2 предложения 3). Если A-модуль M сепарабелен над K, то для любого расширения E поля K $(E \otimes A)$-модуль $E \otimes M$ сепарабелен *над полем* E: действительно, если F — расширение поля E, то $F \otimes_E (E \otimes M)$ и $F \otimes_E (E \otimes A)$ отождествляются соответственно с $F \otimes M$ и $F \otimes A$.

Предложение 5. *Пусть A — алгебра над полем K, и M — A-модуль конечного типа; если существует совершенное поле P, являющееся алгебраическим расширением поля K и такое, что $(P \otimes A)$-модуль $P \otimes M$ без радикала, то модуль M сепарабелен над K.*

Пусть E — произвольное расширение поля K и Ω — алгебраическое замыкание поля E; так как P алгебраично над K, то можно считать, что $P \subset \Omega$. Так как P совершенно, поле Ω является

сепарабельным расширением поля P (гл. V, § 7, n° 3, предложение 4), и следовательно (n° 2, следствие 1 предложения 3), радикал $(\Omega \otimes A)$-модуля $\Omega \otimes M = \Omega \otimes_P (P \otimes M)$ равен нулю. Так как модуль M конечного типа и так как поле Ω алгебраично над E и $\Omega \otimes M = \Omega \otimes_E (E \otimes M)$, предложение 2б) n° 2 показывает, что модуль $E \otimes M$ без радикала, откуда и следует предложение.

Следствие. *Алгебра A над полем K сепарабельна тогда и только тогда, когда существует совершенное поле P, являющееся алгебраическим расширением поля K и такое, что алгебра $P \otimes A$ без радикала.*

Достаточно применить предложение 5 к случаю $M = A_s$.

Замечание. Если алгебра A имеет *конечный ранг* над K, то в предыдущем следствии можно опустить предположение, что поле P *алгебраично* над K. Достаточно повторить доказательство предложения 5, взяв в качестве Ω алгебраически замкнутое расширение поля E, содержащее P, и вместо предложения 2б) n° 2 применить предложение 2в): в самом деле, алгебра $E \otimes A$ имеет над полем E конечный ранг и является, следовательно, *артиновым* кольцом.

Предложение 6. *Пусть A — алгебра над полем K, и M — полупростой A-модуль. Для того чтобы модуль M был сепарабельным над K, необходимо и достаточно, чтобы для любого простого подмодуля модуля M центр его коммутанта был сепарабельным расширением поля K.*

Ввиду замечаний, предшествующих предложению 5, можно ограничиться случаем, когда модуль M прост. Пусть Z — центр тела, коммутанта модуля M, и E — расширение поля K; по теореме 2 n° 4, для того чтобы модуль $E \otimes M$ был без радикала, необходимо и достаточно, чтобы алгебра $E \otimes Z$ была без радикала. Тогда предложение следует из определения 1.

Следствие. *Пусть A — полупростая алгебра над полем K. Для того чтобы A была сепарабельна над K, необходимо и достаточно, чтобы центр любой ее простой компоненты был сепарабельным расширением поля K.*

Это следует из предложения 6, примененного к A_s, и описания центра простого кольца (§ 5, n° 4, теорема 2 и предложение 12).

Определение 2. *Пусть A — алгебра над полем K. A-модуль M называется абсолютно полупростым, если для любого расширения E поля K $(E \otimes A)$-модуль $E \otimes M$ полупрост. Алгебра A называется абсолютно полупростой, если для любого расширения E поля K алгебра $E \otimes A$ полупроста.*

Предложение 7. *Пусть A — алгебра над полем K, и M — A-модуль конечной размерности над K. Модуль M абсолютно полупрост тогда и только тогда, когда он сепарабелен над K.*

Необходимость условия очевидна. Обратно, если это условие выполнено, то для всякого расширения E поля K $(E \otimes A)$-модуль $E \otimes M$ имеет конечную размерность над E и *тем более* конечную длину; так как он без радикала, то он полупрост (§ 6, n° 4, теорема 4).

Следствие. *Конечномерная алгебра над полем A абсолютно полупроста тогда и только тогда, когда она сепарабельна над K* (см. упражнение 9б)).

6. Тензорное произведение с сепарабельным модулем

Теорема 3. *Пусть A, B — алгебры над полем K, $C = A \otimes B$, M — A-модуль, сепарабельный над K, N — B-модуль. Тогда*

$$\mathfrak{R}_C(M \otimes N) \subset M \otimes \mathfrak{R}_B(N). \tag{9}$$

Если, в частности, N — модуль без радикала, то и C-модуль $M \otimes N$ без радикала.

Предположим сначала, что модуль N *прост*; пусть F — коммутант модуля N, и Z — центр F. В силу леммы 2 n° 4 достаточно доказать, что радикал $(A \otimes F^0)$-модуля $M \otimes F_r$ равен нулю. Но $M \otimes F_r$ изоморфен $(M \otimes Z) \otimes_Z F_r$; так как, по предположению, модуль M сепарабелен, то $M \otimes Z$ — модуль без радикала; так как Z — центр тела F, по следствию 1 предложения 3 (n° 2) $M \otimes F_r$ — модуль без радикала.

Перейдем теперь к общему случаю. Пусть $z = \sum_i c_i \otimes y_i$ — элемент радикала $\mathfrak{R}_C(M \otimes N)$, $c_i \in M$, $y_i \in N$; можно считать,

что элементы c_i линейно независимы над полем K. Если N' — простой B-модуль, то, по предыдущему, $M \otimes N'$ — C-модуль без радикала; тогда для любого B-гомоморфизма f модуля N в N' $(1 \otimes f)(z) = \sum_i c_i \otimes f(y_i) = 0$ (§ 6, n° 2, предложение 2), и следовательно, $f(y_i) = 0$ для любого i. Это показывает, что элементы y_i принадлежат радикалу модуля N, что и заканчивает доказательство.

Следствие 1. *Если алгебра A сепарабельна, то для любого B-модуля N справедливо включение* $\mathfrak{R}_C(A \otimes N) \subset A \otimes \mathfrak{R}_B(N)$.

Следствие 2. *Пусть A, B — алгебры над полем K. Если A-модуль M сепарабелен и B-модуль N сепарабелен, то $(A \otimes B)$-модуль $M \otimes N$ сепарабелен.*

Пусть E — расширение поля K; так как модуль N сепарабелен, $N \otimes E$ является модулем без радикала над $B \otimes E$; ввиду теоремы 3 модуль $M \otimes (N \otimes E)$ над алгеброй $A \otimes (B \otimes E)$ будет без радикала. Тогда из ассоциативности тензорного произведения следует, что $(M \otimes N) \otimes E$ — модуль без радикала над алгеброй $(A \otimes B) \otimes E$, что и доказывает следствие.

Следствие 3. *Пусть A, B — алгебры над полем K. Если A сепарабельна, а B без радикала, то $A \otimes B$ без радикала.*

Достаточно в теореме 3 положить $M = A_s$, $N = B_s$.

Следствие 4. *Пусть A, B — алгебры над полем K. Если алгебра $A \otimes B$ полупроста, то A и B полупросты. Обратно, если одна из них сепарабельна и одна или другая имеет конечную размерность над полем K, то алгебра $A \otimes B$ полупроста.*

Первое утверждение следует из теоремы 2а) при $M = A_s$, $N = B_s$. Если A (соответственно B) конечного ранга над полем K, то $A \otimes B$ является B-модулем (соответственно A-модулем) конечного типа; поскольку B (соответственно A) — артиново кольцо, то этот B-модуль (соответственно A-модуль) артинов (§ 2, n° 3, предложение 7). *Тем более* артиновым будет кольцо $A \otimes B$, кроме того, по следствию 3 это кольцо без радикала и, следовательно, полупросто (§ 6, n° 4, следствие 2 теоремы 4).

7. *Простые модули над тензорным произведением алгебр*

Предложение 8. *Пусть A, B — алгебры над полем K, P — простой $(A \otimes B)$-модуль конечной размерности над K. Тогда существуют простой A-модуль M и простой B-модуль N такие, что модуль P изоморфен некоторому фактормодулю $(A \otimes B)$-модуля $M \otimes N$. Кроме того, классы модулей M и N* (§ 3, n° 2) *однозначно определяются классом модуля P.*

Так как модуль P имеет конечную размерность над полем K, то в нем, как в A-модуле, найдется простой A-подмодуль M. Модуль P можно рассматривать и как A-модуль и как B-модуль (при сужении кольца операторов), и гомотетии A-модуля P перестановочны с гомотетиями B-модуля P.

Если P рассматривается как A-модуль, то группа $\mathscr{L}_A(M, P)$ оказывается наделенной структурой B-модуля (гл. III, приложение II, n° 7). Пусть K-линейное отображение φ модуля $M \otimes \mathscr{L}_A(M, P)$ в P определяется равенством $\varphi(x \otimes u) = u(x)$ при $x \in M$, $u \in \mathscr{L}_A(M, P)$; это отображение является $(A \otimes B)$-гомоморфизмом, так как при $a \in A$, $b \in B$, $x \in M$ и $u \in \mathscr{L}_A(M, P)$ выполняется равенство

$$\varphi((a \otimes b)(x \otimes u)) = \varphi((ax) \otimes (bu)) = (bu)(ax) =$$
$$= bu(ax) = b(au(x)) = (a \otimes b)\varphi(x \otimes u).$$

С другой стороны, модуль $\mathscr{L}_A(M, P)$ имеет конечную размерность над K и не сводится к 0; следовательно, у него существует простой B-подмодуль N. Тензорное произведение $M \otimes N$ канонически отождествляется с некоторым подмодулем в $M \otimes \mathscr{L}_A(M, P)$ (гл. III, § 1, n° 3, следствие 3 предложения 7), и сужение гомоморфизма φ на $M \otimes N$ не равно тождественно нулю; следовательно, это сужение сюръективно (§ 4, n° 3, лемма 2), иными словами, модуль P изоморфен фактормодулю модуля $M \otimes N$. Кроме того, $M \otimes N$ является, очевидно, полупростым A-модулем, изотипным типа M, и полупростым B-модулем, изотипным типа N; поэтому, ввиду A-линейности и B-линейности отображения φ, модуль P будет полупростым A-модулем, изотипным типа M, и полупростым B-модулем, изотипным типа N, что и заканчивает доказательство.

Следствие. *Пусть A, B — алгебры над алгебраически замкнутым полем K; пусть $\mathscr{C}(A)$* (соответственно $\mathscr{C}(B)$, $\mathscr{C}(A \otimes B)$) — *множество классов простых модулей над A* (соответственно B, $A \otimes B$), *имеющих конечную размерность над полем K, и $M \in \mathscr{C}(A)$, $N \in \mathscr{C}(B)$. Тогда $M \otimes N$ — простой $(A \otimes B)$-модуль и отображение, которое каждой паре (M, N) ставит в соответствие класс модуля $M \otimes N$, является биекцией произведения $\mathscr{C}(A) \times \mathscr{C}(B)$ на класс $\mathscr{C}(A \otimes B)$.*

По теореме Бернсайда (§ 4, n° 3, следствие 1 предложения 2) коммутанты модулей M и N отождествляются с K, и следовательно, по теореме 2б) модуль $M \otimes N$ прост. Второе утверждение следствия вытекает из предложения 8.

Упражнения. 1) Пусть A, B — алгебры над полем K, и M — абелева группа, наделенная структурой A-модуля и структурой B-модуля. Для любого $a \in A$ (соответственно $b \in B$) через $\varphi(a)$ (соответственно $\psi(b)$) обозначим эндоморфизм группы M, определяемый элементом a (соответственно b). Предположим, что $\varphi(\lambda) = \psi(\lambda)$ для любого $\lambda \in K$ и $\varphi(a)$ и $\psi(b)$ коммутируют при всех $a \in A$ и $b \in B$. Показать, что при этих условиях на M существует единственная структура $(A \otimes B)$-модуля такая, что данные структуры A-модуля и B-модуля получаются из нее сужением кольца скаляров до A и B соответственно.

2) Пусть C — кольцо, и B — подкольцо в C, содержащее его единицу и такое, что всякий максимальный левый идеал кольца B содержится в некотором максимальном левом идеале кольца C. Показать, что при этих условиях справедлива формула (4) из леммы 1.

3) Пусть $B = K[X]$ — алгебра многочленов от одного переменного над полем K, $C = K[[X]]$ — алгебра формальных степенных рядов от одного переменного над K; B рассматривается как подкольцо в C.

а) Показать, что обратный образ радикала модуля C_s при каноническом отображении $y \to 1 \otimes y$ модуля B_s в $C \otimes_B B_s = C_s$ не содержится в радикале модуля B_s (см. § 6, n° 3, примеры 1 и 2).

б) Вывести отсюда, что C не является свободным B-модулем.

4) Пусть B — алгебра $K[X]$ многочленов от одного переменного над полем K, A — ее поле дробей $K(X)$. Показать, что $(A \otimes B)$-модуль A (упражнение 1) прост, но как B-модуль A совпадает со своим радикалом.

5) Пусть A — алгебра $K[X]$ многочленов от одного переменного над полем K, B — алгебра над полем K.

а) Показать, что элемент $1 \otimes 1 - X \otimes y$, где $y \in B$, обратим в $A \otimes B$ тогда и только тогда, когда элемент y нильпотентен.

б) Пусть алгебра B не содержит нильпотентных элементов $\neq 0$. Вывести из а) и предложения 3, что алгебра $A \otimes B$ без радикала. Получить отсюда пример, в котором $\mathfrak{R}(B) \neq \{0\}$, но алгебра $A \otimes B$ без радикала (см. § 6, n° 3, пример 1).

*6) Пусть A — квазипростая алгебра над K (§ 5, упражнение 5), Ω — кольцо эндоморфизмов абелевой группы A.

а) Пусть H_L, H_R — кольца левых и правых умножений алгебры A (§ 1, n° 2), H — подкольцо в Ω, порожденное объединением $H_L \cup H_R$. Показать, что A — простой H-модуль, и вывести из этого, что его центр Z — поле (заметить, что центр Z изоморфен коммутанту подкольца H в Ω).

б) Пусть B — алгебра над полем K. Показать, что всякий двусторонний идеал алгебры $A \otimes B$ имеет вид $A \otimes_Z \mathfrak{b}$, где $\mathfrak{b}$ — двусторонний идеал в $L \otimes B$. (Сначала рассмотреть случай $Z = K$; затем, пользуясь утверждением а), применить предложение 6 § 4, n° 5, так же как в лемме 2 n° 4.)

в) Вывести из б), что если алгебры A и B над K квазипросты и одна из них имеет центр K, то алгебра $A \otimes B$ квазипроста.

г) Пусть B — алгебра над K, A — квазипростая подалгебра в B, центр которой $Z \subset K$. Показать, что A и ее коммутант A' в алгебре B линейно раздельны над Z (использовать б)).

д) Вывести из в) и г), что если алгебра A квазипроста над K, то H_L и H_R линейно раздельны в Ω над своим общим центром Z и кольцо H полупросто. Показать, кроме того, что подкольцо H плотно в $\mathscr{L}_Z(A)$ $H = \mathscr{L}_Z(A)$ тогда и только тогда, когда алгебра A конечного ранга над Z (см. § 5, упражнение 4).

е) Пусть A — полупростая алгебра с центром K. Вывести из д), что алгебра $A \otimes A^0$ полупроста тогда и только тогда, когда ранг $[A : K]$ конечен.

7) Пусть алгебра A имеет нильпотентный радикал $\neq \{0\}$ и ее центр K — поле. Показать, что кольца H_L и H_R левых и правых умножений алгебры A не являются линейно раздельными над своим общим центром в кольце Ω эндоморфизмов абелевой группы A.

8) Пусть E — расширение конечной степени поля K; алгебра $E \otimes E$ полупроста тогда и только тогда, когда расширение E сепарабельно над K (свести доказательство к случаю, когда E — радикальное расширение).

*9) Пусть E — расширение поля K. Для того чтобы алгебра $E \otimes F$ при любом расширении F поля K была полупростой, необходимо и достаточно, чтобы E было радикальным расширением некоторого сепарабельного алгебраического расширения E_0 поля K конечной степени над K. Показать последовательно, что:

а) Поле E не может быть трансцендентным расширением поля K (взять в качестве F чисто трансцендентное расширение поля K, алгебраически раздельное с E, и воспользоваться упражнением 4 гл. V, § 9).

б) Степень $[E_0 : K]$ наибольшего сепарабельного расширения E_0 поля K, содержащегося в E, обязательно конечна (заметить, что в противном случае алгебра $E \otimes F$, где F — наибольшее сепарабельное расширение поля K, содержащееся в алгебраическом замыкании поля K, содержит ортогональные системы идемпотентов с произвольно большим числом элементов).

в) Показать, что, обратно, если степень $[E_0 : K]$ конечна, то при произвольном сепарабельном расширении F поля K алгебра $E_0 \otimes F$ является прямой композицией сепарабельных расширений C_j поля K $(1 \leqslant j \leqslant r)$, а алгебра $E \otimes F$ — прямой композицией радикальных расширений D_j полей C_j $(1 \leqslant j \leqslant r)$.

*10) Пусть V — векторное пространство бесконечной размерности над телом D, A — плотное подкольцо в $\mathscr{L}_D(V)$ и его цоколь $\mathfrak{S}$ не сводится к 0. Пусть K — подполе, лежащее в центре D, B — алгебра над K. Показать, что если радикал алгебры $D^0 \otimes B$ не сводится к 0, то и радикал алгебры $A \otimes B$ не сводится к нулю. (Используя упражнение 31 § 6, свести доказательство к случаю, когда A — алгебра над полем K, порожденная цоколем $\mathfrak{S}$ и единицей. Затем рассмотреть в $\mathfrak{S} \otimes B$ элементы $\sum_i u_i \otimes b_i$, обладающие следующим свойством: пусть M — подпространство конечной размерности в V, содержащее все образы $u_i(V)$, N — его дополнение в V, содержащееся в ядрах эндоморфизмов u_i (см. § 5, упражнение 10з)); отождествим каждый u_i с матрицей его сужения на M относительно некоторого базиса в M; тогда сумма $\sum_i u_i \otimes b_i$ должна отождествиться с матрицей, все элементы которой принадлежат радикалу алгебры $D^0 \otimes B$. Показать, что эти элементы образуют в $\mathfrak{S} \otimes B$ идеал, содержащийся в радикале алгебры $A \otimes B$, и применить упражнение 5 § 6.)

11) Пусть K — поле характеристики 0, A — квазипростая алгебра над K, определенная в упражнении 13 § 5, B — алгебра $K[[T]]$ формальных степенных рядов от одного переменного T над полем K. Показать, что B является центром алгебры $A \otimes B$, алгебра $A \otimes B$ не имеет делителей нуля и что единственными обратимыми элементами этой алгебры будут обратимые элементы алгебры B. Вывести отсюда, что алгебра $A \otimes B$ примитивна, хотя ее центр имеет радикал $\neq \{0\}$ (используя упражнение 6б), показать, что максимальный левый идеал алгебры $A \otimes B$, содержащий элемент $1 \otimes 1 - D \otimes T$ (обозначения из упражнения 13 § 5), не имеет двусторонних идеалов, отличных от $\{0\}$).

12) Пусть K — несовершенное поле, $E \neq K$ — его радикальное расширение, имеющее конечную степень над K. Пусть V — векторное пространство бесконечной размерности над полем E, и A — подалгебра (над K) в $\mathscr{L}_E(V)$, порожденная эндоморфизмами конечного ранга пространства V и тождественным отображением. Показать, что радикал тензорного произведения $A \otimes E$ не сводится к нулю

(см. упражнение 10), хотя центр $A \otimes B$ является полем, изоморфным E.

13) Пусть A, B — простые алгебры над полем K и алгебра B сепарабельна. Предположим, кроме того, что алгебра A имеет конечный ранг над своим центром Z, и Z — алгебраическое расширение поля K. Показать, что кольцо $A \otimes B$ регулярно (§ 6, упражнение 15) (заметить, что всякий элемент алгебры $A \otimes B$ принадлежит некоторой подалгебре вида $A_1 \otimes B$, где A_1 — простая алгебра конечного ранга над полем K). Показать, что этот результат не распространяется на случай, когда Z — трансцендентное расширение поля K (см. § 6, упражнение 17 и гл. V, § 9, упражнение 4).

14) Пусть A, B — алгебры над полем K, M — A-модуль, N — B-модуль, C — алгебра $A \otimes B$. Для любой пары эндоморфизмов $u \in \mathscr{L}_A(M)$, $v \in \mathscr{L}_B(M)$ существует единственный C-эндоморфизм w тензорного произведения $M \otimes N$ такой, что $w(x \otimes y) = u(x) \otimes v(y)$; положив $w = \varphi(u \otimes v)$, получим K-линейное отображение φ произведения $\mathscr{L}_A(M) \otimes \mathscr{L}_B(N)$ в $\mathscr{L}_C(M \otimes N)$ (это отображение называется *каноническим*). Ниже мы будем считать, что A-модуль M *свободен*.

а) Для того чтобы $M \otimes N$ был точным C-модулем, необходимо и достаточно, чтобы B-модуль N был точным (рассмотреть базис алгебры A над K).

б) Показать, что каноническое отображение φ тензорного произведения $\mathscr{L}_A(M) \otimes \mathscr{L}_B(N)$ в $\mathscr{L}_C(M \otimes N)$ инъективно и образ $\varphi(\mathscr{L}_A(M) \otimes \mathscr{L}_B(N))$ является в $\mathscr{L}_C(M \otimes N)$ плотным подкольцом. (Для доказательства первого утверждения рассмотреть элемент $z = \Sigma u_i \otimes v_i$, где $v_i \in \mathscr{L}_B(N)$ линейно независимы над K, и записать, что $\varphi(z)$ аннулируется на всех элементах некоторого базиса модуля M над K. Для доказательства второго утверждения заметить, что, выбрав в M базис (m_λ) над кольцом A и в A базис (a_λ) над полем K, для любого C-эндоморфизма w модуля $M \otimes N$ можно написать равенство $w(m_\lambda \otimes y) = \sum_{\alpha,\mu} (a_\alpha m_\mu) \otimes v_{\alpha\lambda\mu}(y)$, где $v_{\alpha\lambda\mu} \in \mathscr{L}_B(N)$ и при всяком $y \in N$ имеется лишь конечное число пар (α, μ) таких, что $v_{\alpha\lambda\mu}(y) \neq 0$.)

в) Показать, что если кольцо гомотетий B_N плотно в бикоммутанте модуля N, то кольцо гомотетий $C_{M\otimes N}$ плотно в бикоммутанте модуля $M \otimes N$ (тем же методом, что в б)).

г) Показать, что если M имеет конечную размерность *над полем* K (откуда следует, что алгебра A конечного ранга над K), то каноническое отображение φ биективно. Это же верно, если модуль M имеет конечный базис над A и если модуль N конечного типа.

д) Предположим, что существуют элемент $y \in N$ и бесконечная последовательность (v_n) эндоморфизмов B-модуля N такие, что векторное подпространство (над полем K), порожденное в N элемен-

тами $v_n(y)$, бесконечномерно. Показать, что если каноническое отображение φ биективно, то модуль M имеет *конечный* базис над A.

*15) Предположим, что A-модуль M свободен, а B-модуль N прост (обозначения из упражнения 14). Пусть $D = \mathscr{L}_B(N)$ — коммутант B-модуля N.

а) Для того чтобы каноническое отображение φ тензорного произведения $\mathscr{L}_A(M) \otimes \mathscr{L}_B(N)$ в $\mathscr{L}_C(M \otimes N)$ было биективным, необходимо и достаточно, чтобы модуль M имел конечный базис над K или тело D имело конечную размерность над K (см. упражнения 14г) и д)).

б) Показать, что C-модуль $M \otimes N$ полупрост тогда и только тогда, когда полупросто кольцо $A^0 \otimes D$. (Свести доказательство к случаю $M = A_s$; для доказательства необходимости условия, заметив, что контрмодуль тензорного произведения $A_s \otimes N$ свободен, применить упражнение 4 § 4, n° 4; для доказательства достаточности использовать упражнения 14б) и в), а также предложение 4, § 4, n° 4.)

16) Пусть D — тело с центром K, V — векторное пространство над телом D, A — простая алгебра конечного ранга над полем K; тогда алгебра $A^0 \otimes D$ изоморфна алгебре матриц $M(E^0)$ над телом E^0 (n° 4, следствие 2 теоремы 2). Показать, что тензорное произведение $A \otimes \mathscr{L}_D(V)$ изоморфно алгебре $\mathscr{L}_E(W)$, где W — векторное пространство размерности $r \cdot \dim_D V$ над телом E (см. упражнение 14г) и § 4, n° 4, предложение 4).

*17) Пусть A, B — тела, содержащие в центре поле K, M — векторное пространство над A, N — векторное пространство над B, положим $C = A \otimes B$.

а) Пусть $x \in M$, $y \in N$, $x \neq 0$, $y \neq 0$. Показать, что элемент $x \otimes y$ свободен в C-модуле $M \otimes N$ (использовать упражнение 14а) и транзитивность аддитивной группы $\mathscr{L}_A(M)$ (соответственно $\mathscr{L}_B(N)$) на множестве элементов модуля M (соответственно N), отличных от 0).

б) Показать, что C-модуль $M \otimes N$ свободен. (Пусть (m_α) — базис модуля M, (n_β) — базис модуля N; используя тот же метод, что в упражнении а), показать, что сумма C-модулей $C(m_\alpha \otimes n_\beta)$ прямая.)

*18) Предположим, в обозначениях упражнения 14, что кольца A и B примитивны и их цоколи S и T соответственно отличны от 0 (см. § 5, упражнения 5 и 9); пусть E (соответственно F) — коммутант некоторого минимального левого идеала алгебры A (соответственно B). Пусть алгебра $E \otimes F$ простая. Показать, что $C = A \otimes B$ — примитивное кольцо с цоколем $S \otimes T$. (Пусть $\mathfrak{m}$ (соответственно $\mathfrak{n}$) — минимальный левый идеал алгебры A (соответственно B); используя лемму 3 n° 4, показать, что $\mathfrak{m} \otimes \mathfrak{n}$ — изотипный полупростой C-модуль конечной длины. Применить упражнение 14а) и упражнение 5е) § 5.)

*19) Пусть V — векторное пространство над телом D и Ω — кольцо эндоморфизмов абелевой группы V; отождествим D с телом гомотетий пространства V.

а) Показать, что подкольца D и $A = \mathscr{L}_D(V)$ линейно раздельны в Ω над своим общим центром Z (см. упражнение 6г)).

б) Для того чтобы подалгебра DA (изоморфная $D \otimes_Z A$) в Ω совпадала с $\mathscr{L}_Z(V)$, необходимо и достаточно, чтобы тело D было конечного ранга над Z. (Для доказательства необходимости рассмотреть сначала случай, когда V имеет размерность 1 над D, и применить упражнение 6д). Затем рассмотреть в $\mathscr{L}_Z(V)$ подалгебру B, состоящую из Z-эндоморфизмов u пространства V таких, что $u(Dx) \subset Dx$, где $x \neq 0$ — некоторый элемент V. Заметить, что $D \subset B$ и при $\mathscr{L}_Z(V) = DA$ справедливо равенство $B = D(B \cap A)$.)

20) Пусть A — алгебра конечного ранга над K. Показать, что A сепарабельна тогда и только тогда, когда алгебра $A \otimes A^0$ полупроста.

*21) Пусть E — радикальное расширение поля K характеристики $p > 0$. Показать, что кольцо $E \otimes E$ нетерово тогда и только тогда, когда степень $[E : K]$ конечна. Заметить, что элемент $x \otimes 1 - 1 \otimes x$, где $x \in E$, нильпотентен; последовательно доказать, что:

а) Если не существует целого числа k такого, что $E \subset K^{p^{-k}}$, то для любого целого числа $n > 0$ существует элемент $z_n \in E \otimes E$ такой, что $z_n^{p^n} = 0$, $z_n^{p^{n-1}} \neq 0$.

б) Пусть $F = K(E^p)$ и $(a_i)_{i \in I}$ — p-базис поля E (гл. V, § 9, упражнение 1в)). Положим $b_i = a_i \otimes 1$, $c_i = a_i \otimes 1 - 1 \otimes a_i$ и для любого отображения φ множества I в $J = [0, p-1]$, равного нулю для всех индексов, кроме конечного числа, через b_φ (соответственно c_φ) обозначим произведение $\prod_i b_i^{\varphi(i)}$ (соответственно $\prod_i c_i^{\varphi(i)}$). Элементы $b_\varphi c_\psi$, где φ и ψ пробегают множество $J^{(I)}$, образуют базис алгебры $E \otimes_F E$ над F. Заметить, наконец, что алгебра $E \otimes_F E$ изоморфна (как алгебра над K) некоторой факторалгебре алгебры $E \otimes_K E$, и использовать упражнение 2б) гл. V, § 8.

*22) Пусть E — алгебраическое расширение поля K. Для того чтобы кольцо $E \otimes E$ было нетеровым, необходимо и достаточно, чтобы степень $[E : K]$ была конечной (используя рассуждение из упражнения 9б), свести доказательство к случаю, когда расширение E радикальное, и применить упражнение 21).

*23) Пусть A, B — алгебры над полем K.

а) Пусть кольцо $A \otimes B$ артиново. Показать, что кольца A и B артиновы.

б) Предположим, что для любой артиновой алгебры B алгебра $A \otimes B$ артинова. Показать, что размерность $[A : K]$ конечна. (Сначала, пользуясь упражнениями 9 и 21, рассмотреть случай, когда алгебра A полупростая. Затем, используя а), установить, что $\mathfrak{R}(A)^k/\mathfrak{R}(A)^{k+1}$ является модулем конечной длины над $A/\mathfrak{R}(A)$.)

24) а) Пусть A — алгебра над полем K, $B = K[X_\iota]_{\iota \in I}$ — алгебра многочленов над K. Показать, что если алгебра A без делителей нуля, то и $A \otimes B$ не имеет делителей нуля.

б) Пусть D — тело конечного ранга над K, и E — чисто трансцендентное расширение поля K; вывести из а), что $D \otimes E$ — тело.

§ 8. Применения: I. Композиции расширений

В этом параграфе остаются в силе соглашения, принятые в начале § 7.

Определение 1. *Пусть E, F — расширения поля K. Композицией (L, u, v) расширений E и F называется расширение L поля K, наделенное дополнительной структурой, определяемой заданием таких K-изоморфизмов u поля E и v поля F на подполя в L, что $u(E)$ и $v(F)$ порождают L.*

Согласно общим определениям (Теор. мн., гл. IV, § 1) *изоморфизм* некоторой композиции (L, u, v) расширений E и F на композицию (L', u', v') расширений E и F есть K-изоморфизм φ поля L на L' такой, что $u' = \varphi_0 u$ и $v' = \varphi_0 v$.

Пусть (L, u, v) — композиция расширений E и F; отображение $(x, y) \to u(x)\, v(y)$ произведения $E \times F$ в L K-билинейно, и следовательно, существует единственное K-линейное отображение w тензорного произведения $E \otimes F$ в L такое, что $w(x \otimes y) = u(x)\, v(y)$ (гл. III, § 1, n° 2); легко проверить, что w будет изоморфизмом *алгебры* $E \otimes F$ в L (гл. III, § 3, n° 1); гомоморфизм w *в этом параграфе* для краткости будет обозначаться через $u \cdot v$.

Предложение 1. *Пусть E, F — расширения поля K.*

а) *Пусть (L, u, v) — композиция E и F, и $\mathfrak{p}$ — ядро гомоморфизма $u \cdot v$: $E \otimes F \to L$. Тогда $(E \otimes F)/\mathfrak{p}$ — кольцо целостности. Пусть L' — поле дробей кольца $(E \otimes F)/\mathfrak{p}$, u' и v' — сужения на E и F канонического гомоморфизма $E \otimes F$ на $(E \otimes F)/\mathfrak{p}$; тогда композиция (L', u', v') расширений E и F изоморфна (L, u, v).*

б) *Обратно, пусть $\mathfrak{q}$ — идеал кольца $E \otimes F$ такой, что $(E \otimes F)/\mathfrak{q}$ — кольцо целостности; тогда существует композиция (L, u, v) расширений E и F (единственная с точностью до изоморфизма) такая, что идеал $\mathfrak{q}$ является ядром гомоморфизма $u \cdot v$.*

Ясно, что если (L, u, v) — композиция расширений E и F, то образ произведения $E \otimes F$ при отображении $w = u \cdot v$ содержится в L, то есть является кольцом целостности, изоморфным $(E \otimes F)/\mathfrak{p}$. Обратно, пусть $\mathfrak{q}$ — идеал в $E \otimes F$ и $A = (E \otimes F)/\mathfrak{q}$ —

кольцо целостности; пусть, далее, L' — поле дробей кольца A, u' и v' — сужения на $u'(E)$ и $v'(F)$ канонического гомоморфизма кольца $E \otimes F$ на A; u' и v' являются K-изоморфизмами, и $u'(E)$ и $v'(F)$ порождают кольцо A, а следовательно, и поле L'. Наконец, пусть (L, u, v) — еще одна композиция расширений E и F такая, что $\mathfrak{q}$ является ядром гомоморфизма $w = u \cdot v$; существует такой изоморфизм φ кольца A на $w(E \otimes F)$, что $u \cdot v = \varphi \circ (u'v')$; изоморфизм φ можно продолжить до K-изоморфизма $\bar{\varphi}$ поля L' на поле дробей $L_1 \subset L$ кольца $w(E \otimes F)$ (гл. I, § 9, n° 4, предложение 4); так как $u(E)$ и $v(F)$ порождают L, то $L_1 = L$, и следовательно, $\bar{\varphi}$ — изоморфизм композиции (L', u', v') на (L, u, v). Это заканчивает доказательство предложения 1.

Замечания. 1) Из определений сразу же следует, что если идеалы $\mathfrak{q}$ и $\mathfrak{q}'$ кольца $E \otimes F$ различны и факторкольца $(E \otimes F)/\mathfrak{q}$ и $(E \otimes F)/\mathfrak{q}'$ являются кольцами целостности, то соответствующие *композиции расширений* не изоморфны (хотя они могут быть изоморфны как *расширения* поля K).

2) Идеал $\mathfrak{p}$ коммутативного кольца A называется простым, если $A/\mathfrak{p}$ — кольцо целостности. Позже мы увидим, что эти идеалы играют большую роль в изучении коммутативных колец.

Предложение 2. *Пусть Ω — алгебраически замкнутое расширение поля K, $E \subset \Omega$ и F — расширения поля K; предположим, что Ω имеет базис трансцендентности над E, кардинальное число которого не меньше кардинального числа базиса трансцендентности поля F над K. Тогда всякая композиция расширений E и F изоморфна некоторой композиции вида $(G_w, 1, w)$, где w — K-изоморфизм поля F на некоторое подполе в Ω, G_w — подполе, порожденное в Ω подполями E и $w(F)$, и 1 — тождественное отображение поля E.*

В самом деле, пусть B — базис трансцендентности поля F над K, и (L, u, v) — композиция расширений E и F. Всякий элемент из $v(F)$ алгебраичен над подполем M, порожденным в L образами $u(E)$ и $v(B)$; следовательно (гл. V, § 3, n° 2, предложение 6), поле L алгебраично над M и имеет базис трансцендентности над $u(E)$, содержащийся в $v(B)$. По условию, наложенному на Ω, изоморфизм u^{-1} поля $u(E)$ на E продолжается до изоморфизма φ поля L на некоторое подполе в Ω (гл. V, § 6, n° 1, предложение 1).

Положив $w = \varphi \circ v$ и $G_w = \varphi(L)$, убеждаемся, что φ является изоморфизмом композиций (L, u, v) и $(G_w, 1, w)$.

Следствие 1. *Если расширение F имеет конечную степень n над K, то существует не более n попарно неизоморфных композиций расширений E и F.*

В самом деле, имеется не более n K-изоморфизмов поля F на подполя в Ω (гл. V, § 7, n° 5, предложение 8).

Следствие 2. *Пусть E — нормальное расширение поля K, и F — расширение K, содержащееся в E. Тогда всякая композиция расширений E и F изоморфна некоторой композиции вида $(E, 1, v)$, где v — K-изоморфизм поля F на некоторое подполе поля E.*

В самом деле, пусть Ω — алгебраическое замыкание поля E; всякий K-изоморфизм поля F на некоторое подполе в Ω отображает F на подполе в E (гл. V, § 6, n° 3, предложение 7); так как поле F алгебраично над K, то можно применить предложение 2.

Предложение 3. *Пусть E, F — расширения поля K, одно из которых сепарабельно над K и одно имеет конечную степень над K. Пусть (L_i, u_i, v_i) — попарно неизоморфные композиции расширений E и F такие, что всякая композиция расширений E и F изоморфна одной из них $(1 \leqslant i \leqslant m)$. Тогда гомоморфизм $(u_i v_i)_{1 \leqslant i \leqslant m}$ кольца $E \otimes F$ в произведении колец $\prod_{i=1}^{m} L_i$ биективен.*

В самом деле (§ 7, n° 6, следствие 4 теоремы 3), кольцо $E \otimes F$ полупросто и является, следовательно, прямой композицией полей G_i (§ 6, n° 4, предложение 9); его идеалы поэтому являются прямыми суммами некоторых G_i (гл. I, § 8, n° 10, предложение 6); пусть $\mathfrak{p}$ — такой идеал. $(E \otimes F)/\mathfrak{p}$ будет кольцом целостности тогда и только тогда, когда идеал $\mathfrak{p}$ имеет вид $\sum_{j \neq i} G_j$ (гл. I, § 8, n° 11, предложение 8), и в этом случае $(E \otimes F)/\mathfrak{p}$ изоморфно G_i. Следовательно, предложение вытекает из предложения 1.

Предложение 4. *Пусть E — расширение Галуа конечной степени поля K, Γ — его группа Галуа, F — алгебра над полем E. Рассмотрим на $E \otimes_K F$ структуру E-алгебры, получающуюся из структуры E-алгебры F. E-линейное отображение w алгебры*

$E \otimes_K F$ на произведение F^Γ такое, что $w(x \otimes y) = (\sigma(x)\, y)_{\sigma\in\Gamma}$, является изоморфизмом E-алгебр. Пусть, кроме того, группа Γ действует на $E \otimes_K K$ и на F^Γ согласно формулам $\sigma(x \otimes y) = \sigma(x) \otimes y$ $(x \in E,\ y \in F,\ \sigma \in \Gamma)$ и $\sigma((a_\tau)_{\tau\in\Gamma}) = (a_{\tau\sigma})_{\tau\in\Gamma}$ $(a_\tau \in F,\ \sigma \in \Gamma)$. Тогда $w \circ \sigma = \sigma \circ w$ для любого $\sigma \in \Gamma$.

Предположим сначала, что $F = E$; по следствию 2 предложения 2 всякая композиция расширений E и F изоморфна некоторой композиции вида $(E, 1, \sigma)$, где $\sigma \in \Gamma$; тогда предложение непосредственно вытекает из предложения 3.

Перейдем к общему случаю; алгебру F можно канонически отождествить с $E \otimes_E F$; тогда $E \otimes_K F$ отождествляется с $E \otimes_K (E \otimes_E F)$ и, следовательно, с $(E \otimes_K E) \otimes_E F$ (гл. III, приложение II, n°n° 4 и 9); элемент $(x \otimes x') \otimes y$, где $x \in E$, $x' \in E$, $y \in F$, отождествляется при этом с $x \otimes (x'y)$. Аналогично F^Γ отождествляется с $(E^\Gamma) \otimes_E F$, причем элемент $((x_\sigma)_{\sigma\in\Gamma}) \otimes y$ последнего произведения отождествляется с элементом $(x_\sigma y)_{\sigma\in\Gamma}$ в F^Γ. Теперь достаточно применить первую часть доказательства.

Замечание. Более общим образом, если F — E-модуль, то аналогично определяется изоморфизм w E-модуля $E \otimes_K F$ на произведение F^Γ, такой, что $w \circ \sigma = \sigma \circ w$ для любого $\sigma \in \Gamma$.

Упражнения. 1) Пусть E — расширение поля K, и Ω — алгебраически замкнутое расширение поля E. Показать, что следующие условия эквивалентны: 1° E — радикальное расширение поля K; 2° при любом расширении F поля K в $E \otimes F$ имеется только один простой идеал; 3° при любом расширении F поля K любые две композиции расширений E и F изоморфны; 4° в $E \otimes \Omega$ имеется единственный простой идеал; 5° любые две композиции расширений E и Ω изоморфны.

2) Пусть K — поле, p — его характеристическая экспонента, Ω — алгебраически замкнутое расширение поля K, $L \subset \Omega$ — расширение поля K, и $\overline{K}$ — алгебраическое замыкание поля K в Ω.

а) Показать, что поля $\overline{K}$ и $L^{p^{-\infty}}$ линейно раздельны над своим пересечением N (рассмотреть первичное линейное соотношение с коэффициентами из $\overline{K}$ между элементами a_λ некоторого базиса (a_λ) поля $L^{p^{-\infty}}$ над N и применить к этому соотношению L-автоморфизм поля Ω).

б) Вывести из а), что всякий K-автоморфизм поля $\overline{K}$, сужение которого на $L \cap \overline{K}$ является тождественным отображением, может быть продолжен до L-автоморфизма поля Ω.

3) а) Пусть K — поле, E, F — его расширения такие, что E алгебраично над K, и K алгебраически замкнуто в F. Показать, что

любые две композиции расширений E и F изоморфны (использовать упражнение 2б)).

б) Пусть E, F — расширения поля K и K алгебраически замкнуто в F. Показать, что если композиции (L, u, v) и (L', u', v') таковы, что $u(E)$ и $v(F)$ (соответственно $u'(E)$ и $v'(F)$) алгебраически раздельны над K, то эти композиции изоморфны. (Сначала, используя предложение 11 гл. V, § 5, n° 4, рассмотреть случай, когда E — чистое расширение поля K; затем применить а) и утверждение 8 гл. V, § 6.)

4) Пусть E, F — расширения поля K и S (соответственно T) — наибольшее сепарабельное алгебраическое расширение поля K, содержащееся в E (соответственно в F). Предположим, что все композиции расширений S и T изоморфны. Показать, что если композиции (L, u, v) и (L', u', v') расширений E и F таковы, что $u(E)$ и $v(F)$ (соответственно $u'(E)$ и $v'(F)$) алгебраически раздельны над K, то эти композиции изоморфны (свести доказательство к случаям, рассмотренным в упражнениях 1 и 3б)).

5) Пусть Ω — алгебраическое замыкание поля K, f и g — сепарабельные неприводимые многочлены из кольца $K[X]$, α — корень многочлена f в Ω, β — корень многочлена g в Ω. Положим $E = K(\alpha)$, $F = K(\beta)$. Пусть $f = f_1 f_2 \dots f_r$ — разложение многочлена f на неприводимые множители в $F[X]$, $g = g_1 g_2 \dots g_s$ — разложение многочлена g на неприводимые множители в $E[X]$. Показать, что $r = s$. Далее, пусть m (соответственно n) — степень f (соответственно g), m_i (соответственно n_j) — степень f_i (соответственно g_j); тогда можно так переставить множители g_j, что $m_i/n_i = m/n$ для всех $1 \leqslant i \leqslant r$ (рассмотреть алгебру $E \otimes F$).

6) Пусть A — кольцо. Двусторонний идеал $\mathfrak{p}$ кольца A называется *простым*, если для любых двусторонних идеалов $\mathfrak{b}$ и $\mathfrak{c}$ кольца A включение $\mathfrak{bc} \subset \mathfrak{p}$ влечет $\mathfrak{b} \subset \mathfrak{p}$ или $\mathfrak{c} \subset \mathfrak{p}$.

а) Показать, что если кольцо A коммутативно, то это определение совпадает с данным после предложения 1.

б) Двусторонний идеал $\mathfrak{p}$ кольца A является простым тогда и только тогда, когда для любых элементов $b \overline{\in} \mathfrak{p}$, $c \overline{\in} \mathfrak{p}$ существует элемент $x \in A$ такой, что $bxc \overline{\in} \mathfrak{p}$ (рассмотреть двусторонние идеалы, порожденные элементами b и c).

*7) а) Пусть A — кольцо, $\mathfrak{a}$ — его двусторонний идеал и $A/\mathfrak{a}$ не содержит нильпотентных идеалов. Показать, что для любого двустороннего идеала $\mathfrak{b} \supset \mathfrak{a}$ и такого, что $\mathfrak{b} \neq \mathfrak{a}$, существует простой идеал (упражнение 6) $\mathfrak{p}$ такой, что $\mathfrak{a} \subset \mathfrak{p}$ и $\mathfrak{b} \not\subset \mathfrak{p}$. (Индукцией по n показать, что существуют две бесконечные последовательности (b_n), (c_n) элементов кольца A такие, что $b_n \in \mathfrak{b}$, $b_n \overline{\in} \mathfrak{a}$ и $b_{n+1} = b_n c_n b_n$. Показать, что максимальный элемент $\mathfrak{p}$ множества двусторонних идеалов, содержащих $\mathfrak{a}$ и не содержащих ни одного b_n, является простым идеалом.)

б) Вывести из а), что наименьший нильрадикал $\mathfrak{C}$ кольца A (§ 6, упражнение 3д)) является пересечением его простых идеалов.

8) Двусторонний идеал $\mathfrak{a}$ кольца A называется *примитивным*, если факторкольцо $A/\mathfrak{a}$ примитивно (§ 5, упражнение 5).

а) Показать, что всякий примитивный идеал — простой (упражнение 6).

б) Пусть $(\mathfrak{a}_\lambda)$ — семейство примитивных идеалов кольца A. Элемент $x \in A$ обратим тогда и только тогда, когда его образ в каждом из колец $A/\mathfrak{a}_\lambda$ обратим (показать, что при выполнении этого условия элемент x не содержится ни в каком максимальном левом идеале).

в) Пусть $\mathfrak{b}$ — левый идеал кольца A, и $\mathfrak{b} + \mathfrak{a}_\lambda = A$ для любого λ. Показать, что $\mathfrak{b} = A$ (в противном случае рассмотреть максимальный левый идеал $\mathfrak{m}$, содержащий $\mathfrak{b}$ и аннулятор A-модуля $A/\mathfrak{m}$).

г) Пусть E — такой A-модуль конечного типа, что $\mathfrak{a}_\lambda E = E$ для любого λ. Показать, что $E = \{0\}$ (используя в), провести индукцию по наименьшему числу образующих модуля E).

д) Пусть E — нетеров A-модуль, и F — пересечение подмодулей $\mathfrak{s}E$, где $\mathfrak{s}$ пробегает множество конечных произведений $\mathfrak{a}_{\lambda_1}\mathfrak{a}_{\lambda_2}\ldots\mathfrak{a}_{\lambda_m}$ примитивных двусторонних идеалов. Показать, что $F = \{0\}$ (использовать г)).

§ 9. Применения: II. Полупростые семейства эндоморфизмов векторного пространства

В этом параграфе через V обозначается векторное пространство конечной размерности над полем K.

1. Полупростые семейства эндоморфизмов векторного пространства

Пусть $\mathfrak{F}$ — некоторое множество эндоморфизмов пространства V, и A — подалгебра в $\mathfrak{L}_K(V)$, порожденная $\mathfrak{F}$ (и единицей 1); так как $\mathfrak{L}_K(V)$ конечномерно над K, то A — *артиново* кольцо. Следующие свойства эквивалентны:

а) алгебра A полупроста;

б) A-модуль V полупрост;

в) всякое подпространство в V, стабильное относительно всех эндоморфизмов $u \in \mathfrak{F}$, обладает дополнением, устойчивым относительно всех $u \in \mathfrak{F}$.

В самом деле, эквивалентность б) и в) следует из того, что подпространства V, устойчивые относительно всех эндоморфизмов $u \in \mathfrak{F}$, являются подмодулями A-модуля V. Ясно, что а) влечет б)

(§ 5, n° 1, определение 1); с другой стороны, модуль V точен, и по предложению 3 § 5, n° 1, из б) следует, что A полупроста: в самом деле, V конечномерно над K, и следовательно, контрмодуль A-модуля V есть модуль конечного типа.

Определение 1. *Множество $\mathfrak{F}$ эндоморфизмов пространства V называется полупростым, если удовлетворяются указанные эквивалентные условия*), 5), в).

Семейство эндоморфизмов пространства V называется *полупростым*, если множество эндоморфизмов этого семейства полупросто; эндоморфизм u пространства V называется *полупростым*, если множество $\{a\}$ полупросто.

Предложение 1. *Для того чтобы эндоморфизм u пространства V был полупрост, необходимо и достаточно, чтобы его минимальный многочлен f не имел кратных множителей.*

В самом деле, алгебра A, порожденная эндоморфизмом u, изоморфна $K[X]/(f)$ (гл. VII, § 5, n° 1), и доказываемое утверждение следует из предложения 8 § 6, n° 3.

Предложение 2. *Пусть $\mathfrak{F}$ — полупростое множество эндоморфизмов пространства V, попарно перестановочных между собой. Тогда всякое подмножество $\mathfrak{F}$ полупросто.*

Алгебра A, порожденная множеством $\mathfrak{F}$, коммутативна, полупроста и имеет конечный ранг над полем K; поэтому предложение вытекает из следствия 3 к предложению 9 § 6, n° 4.

2. *Абсолютно полупростые семейства эндоморфизмов векторного пространства*

Пусть L — расширение поля K. Для любого эндоморфизма u пространства V через $u_{(L)}$ обозначим эндоморфизм векторного пространства $V_{(L)} = L \otimes_K V$, получающийся из u расширением поля скаляров (гл. III, § 2, n° 2, теорема 1); для любого множества $\mathfrak{F}$ эндоморфизмов пространства V обозначим через $\mathfrak{F}_{(L)}$ множество элементов $u_{(L)}$, где u пробегает $\mathfrak{F}$. Так как $u_{(L)} = 1 \otimes u$, подалгебра, порожденная в $\mathscr{L}_L(V_{(L)})$ множеством $\mathfrak{F}$, отождествляется с $L \otimes_K A$, где A — подалгебра в $\mathscr{L}_K(V)$, порожденная множеством $\mathfrak{F}$.

ПРЕДЛОЖЕНИЕ 3. *Пусть* $\mathfrak{F}$ *— некоторое множество эндоморфизмов пространства* V, L *— расширение поля* K.

а) *Если множество* $\mathfrak{F}_{(L)}$ *полупросто, то* $\mathfrak{F}$ *полупросто.*

б) *Если* $\mathfrak{F}$ *полупросто и* L *сепарабельно над* K, *то* $\mathfrak{F}_{(L)}$ *полупросто.*

Из предыдущих замечаний ясно, что а) вытекает из следствия к предложению 2 § 7, n° 2, а б) вытекает из следствия 1 к предложению 3 § 7, n° 2.

ОПРЕДЕЛЕНИЕ 2. *Множество* $\mathfrak{F}$ *эндоморфизмов пространства* V *называется абсолютно полупростым, если при любом расширении* L *поля* K *множество* $\mathfrak{F}_{(L)}$ *полупросто.*

Семейство эндоморфизмов пространства V называется *абсолютно полупростым*, если множество элементов этого семейства абсолютно полупросто; эндоморфизм u пространства V называется *абсолютно полупростым*, если множество $\{u\}$ абсолютно полупросто, другими словами, эндоморфизм $u_{(L)}$ полупрост для любого расширения L поля K.

Следующие условия, очевидно, эквивалентны:

а) множество $\mathfrak{F}$ абсолютно полупросто;

б) подалгебра A, порожденная в $\mathscr{L}_K(V)$ множеством $\mathfrak{F}$, абсолютно полупроста (§ 7, n° 5, определение 2; это показывает, что в случае, когда $\mathfrak{F}$ — алгебра над полем K, то определение 2 совпадает с определением 2 § 7, n° 5);

в) A-модуль V абсолютно полупрост (см. § 7, n° 5, определение 2).

ПРЕДЛОЖЕНИЕ 4. *Для того чтобы множество* $\mathfrak{F}$ *эндоморфизмов пространства* V *было абсолютно полупростым, необходимо и достаточно, чтобы существовало совершенное расширение* P *поля* K, *для которого множество* $\mathfrak{F}_{(P)}$ *полупросто.*

Так как алгебра A конечного ранга над K, то, ввиду предыдущих замечаний, это вытекает из следствия предложения 7 и замечания после предложения 5 § 7, n° 5.

ПРЕДЛОЖЕНИЕ 5. *Для того чтобы эндоморфизм и пространства* V *был абсолютно полупростым, необходимо и достаточно, чтобы его минимальный многочлен имел в алгебраическом замыкании* Ω *поля* K *только простые корни.*

В самом деле, при любом расширении L поля K минимальный многочлен f эндоморфизма u совпадает с минимальным многочленом эндоморфизма $u_{(L)}$ (гл. VII, § 5, n° 1, следствие 2 предложения 2); условие, что многочлен f не имеет кратных множителей, из $\Omega[X]$, означает, что все его корни в Ω простые, откуда следует, что при любом расширении L поля K многочлен f не будет иметь в $L[X]$ кратных множителей. Доказываемое утверждение вытекает тогда из предложения 1.

Теорема 1. *Пусть $\mathfrak{F}$ — множество эндоморфизмов пространства V, попарно перестановочных между собой, A — подалгебра в $\mathfrak{L}_K(V)$, порожденная множеством $\mathfrak{F}$. Следующие свойства эквивалентны:*

а) *A — прямая композиция конечного числа сепарабельных расширений поля K;*

б) *$\mathfrak{F}$ абсолютно полупросто;*

в) *всякий элемент множества $\mathfrak{F}$ абсолютно полупрост.*

Эквивалентность а) и б) вытекает из следствия предложений 6 и 7 § 7, n° 5. Из предложения 2 следует, что б) влечет в). Обратно, предположим, что всякий элемент множества $\mathfrak{F}$ абсолютно полупрост; так как алгебра A конечномерна над K, то она порождается конечным числом элементов u_j $(1 \leqslant j \leqslant m)$ множества $\mathfrak{F}$. Пусть Ω — алгебраическое замыкание поля K, B_j $(1 \leqslant j \leqslant m)$ — подалгебра в $\Omega \otimes_K A$, порожденная элементом $(u_j)_{(\Omega)}$; алгебры B_j абсолютно полупросты, так что их тензорное произведение P над полем Ω полупросто (§ 7, n° 5, следствие предложения 7 и n° 6, следствие 4 теоремы 3). Так как алгебра $\Omega \otimes_K A$ коммутативна и порождается объединением B_j, то существует канонический гомоморфизм тензорного произведения P на $\Omega \otimes_K A$ (гл. III, § 3, n° 3); алгебра $\Omega \otimes_K A$ изоморфна тогда факторалгебре полупростой алгебры и, следовательно, полупроста (§ 5, n° 3, предложение 10); ввиду предложения 4 отсюда следует, что в) влечет б).

Следствие. *Сумма и произведение двух абсолютно полупростых перестановочных эндоморфизмов абсолютно полупросты.*

Сумма или произведение двух абсолютно полупростых эндоморфизмов, не перестановочных между собой, не обязательно абсолютно полупросты (упражнение 2).

3. *Диагонализируемые семейства эндоморфизмов векторного пространства*

Определение 3. *Множество $\mathfrak{F}$ эндоморфизмов пространства V называется диагональным относительно базиса (e_i) пространства V, если матрицы всех $u \in \mathfrak{F}$ относительно базиса (e_i) диагональны. Множество $\mathfrak{F}$ называется диагонализируемым, если существует такой базис (e_i), относительно которого множество $\mathfrak{F}$ диагонально.*

Семейство эндоморфизмов называется *диагонализируемым*, если множество эндоморфизмов этого семейства диагонализируемо; эндоморфизм u называется *диагонализируемым* *), если множество $\{u\}$ диагонализируемо. Для того чтобы эндоморфизм u был диагонализируемым, *необходимо и достаточно, чтобы все корни его минимального многочлена лежали в поле K и были простыми* (гл. VII, § 5, n° 4, предложение 10).

Всякое диагонализируемое множество $\mathfrak{F}$ состоит из попарно перестановочных эндоморфизмов и, следовательно, по теореме 1 n° 2 абсолютно полупросто.

Предложение 6. *Пусть $\mathfrak{F}$ — некоторое множество эндоморфизмов пространства V, A — подалгебра, порожденная в $\mathscr{L}_K(V)$ множеством $\mathfrak{F}$. Следующие свойства эквивалентны:*

а) *A изоморфна некоторой алгебре вида K^r;*

б) *множество $\mathfrak{F}$ диагонализируемо;*

в) *все элементы множества $\mathfrak{F}$ диагонализируемы и попарно перестановочны.*

Прежде всего, а) влечет б): алгебра A полупроста, A-модуль V является прямой суммой простых A-модулей V_i, которые должны быть изоморфны простым компонентам алгебры A (рассматриваемым как A-модули; см. § 5, n° 3, предложение 11 и n° 4, теорема 2) и, следовательно, имеют размерность 1 над K. Ясно, что б) влечет в). Докажем, наконец, что в) влечет а): алгебра A конечномерна над K и порождается поэтому конечным числом элементов u_j $(1 \leqslant j \leqslant m)$ множества $\mathfrak{F}$. Пусть B_j — подалгебра, порожденная в A элементом u_j; она изоморфна факторалгебре $K[X]/(f_j)$, где f_j — минимальный многочлен эндоморфизма u_j. Из наших

*) Это понятие мы определили уже в гл. VII, § 5, n° 4, под названием «эндоморфизм, приводимый к диагональному виду».

предположений следует тогда, что алгебра B_j изоморфна некоторой алгебре вида K^r (гл. VII, § 1, n° 2, предложение 4); это же справедливо и для тензорного произведения P алгебр B_j (гл. III, § 3, n° 1). Так как алгебра A коммутативна и порождается объединением B_j, то существует канонический гомоморфизм алгебры P на A (гл. III, § 3, n° 3), и следовательно, A будучи изоморфной факторалгебре алгебры вида K^r, сама имеет такой вид (гл. I, § 8, n° 10).

Предложение 7. *Пусть $\mathfrak{F}$ — некоторое множество эндоморфизмов пространства V. Следующие свойства эквивалентны:*

а) *существует расширение Галуа N конечной степени поля K такое, что множество $\mathfrak{F}_{(N)}$ диагонализируемо;*

б) *существует расширение L поля K такое, что множество $\mathfrak{F}$ диагонализируемо;*

в) *множество $\mathfrak{F}$ абсолютно полупросто, и его элементы попарно перестановочны.*

Ясно, что а) влечет б). Пусть условие б) выполнено и Ω — алгебраическое замыкание поля K; тогда множество $F_{(\Omega)}$ диагонализируемо, следовательно, полупросто, так что (предложение 4, n° 2) множество $\mathfrak{F}$ абсолютно полупросто. Наконец, предположим, что выполняется условие в); пусть A — подалгебра в $\mathfrak{F}_K(V)$, порожденная множеством $\mathfrak{F}$, и Ω — алгебраическое замыкание поля K; так как A конечномерна над K, то она порождается конечным числом элементов u_j $(1 \leqslant j \leqslant m)$ множества $\mathfrak{F}$ и эндоморфизмы u_j абсолютно полупросты (n° 2, теорема 1). Корни минимальных многочленов эндоморфизмов u_j $(1 \leqslant j \leqslant m)$ в поле Ω принадлежат одному и тому же расширению Галуа N конечной степени поля K (гл. V, § 6, n° 3, следствие 3 предложения 9 и § 7, n° 6, предложение 10). Следовательно, эндоморфизмы $(u_j)_{(N)}$ диагонализируемы и для завершения доказательства достаточно применить предложение 6.

4. *Полупростые и нильпотентные компоненты эндоморфизма*

Предложение 8. *Пусть поле K совершенно. Всякий эндоморфизм u пространства V единственным способом может быть представлен в виде $u = u_s + u_n$, где u_s и u_n — перестановочные эндоморфизмы пространства V, u_s (абсолютно) полупрост* (см.

предложение 4), *а* u_n *нильпотентен; более того, эндоморфизмы* u_s *и* u_n *являются многочленами от* u *с коэффициентами из поля* K *и без свободного члена.*

Существование и единственность эндоморфизмов u_s и u_n следуют из предложений 11 и 12 гл. VII, § 5, n° 4. Эти предложения показывают также, что в пространстве V существует базис (e_i), относительно которого матрицы U_s и U_n эндоморфизмов u_s и u_n являются линейными комбинациями степеней матрицы U эндоморфизма u относительно (e_i) с коэффициентами из алгебраического замыкания Ω поля K. Так как все элементы матриц U, U_s и U_n лежат в K, то U_s и U_n являются также линейными комбинациями степеней матрицы U с коэффициентами *из поля* K (гл. II, § 5, n° 3, теорема 1); иными словами, матрицы U_s и U_n являются многочленами $P(U)$ и $Q(U)$, где P и Q принадлежат $K[X]$. Остается доказать, что можно подобрать многочлены P и Q без свободного члена, причем достаточно доказать это для Q. Если эндоморфизм u обратим, то его характеристический многочлен имеет ненулевой свободный член; тогда по теореме Гамильтона — Кэли (гл. VII, § 5, n° 3, следствие 2 предложения 8) 1 является многочленом от u без свободного члена, откуда в рассматриваемом случае и следует наше утверждение. Если эндоморфизм u необратим, то его ядро W не сводится к 0 и устойчиво относительно u_n (гл. VII, § 5, n° 4, лемма 2). Так как сужение эндоморфизма u_n на W нильпотентно, то существует ненулевой вектор $x \in W$ такой, что $u(x) = u_n(x) = 0$, откуда следует, что многочлен Q не может иметь свободного члена.

Следствие. *Пусть* u, v *— перестановочные эндоморфизмы пространства* V. *Тогда эндоморфизмы* u, v, u_s, v_s, u_n, v_n *попарно перестановочны.*

Определение 4. *Эндоморфизмы* u_s *и* u_n, *определенные в предложении* 8, *называются соответственно полупростой и нильпотентной компонентами эндоморфизма* u.

Предложение 9. *Предположим, что поле* K *совершенно. Пусть* u *— эндоморфизм пространства* V, W *— подпространство в* V, *устойчивое относительно* u, u' *— сужение* u *на* W, u'' *— эндоморфизм пространства* V/W, *получаемый из* u *путем факторизации.*

Тогда полупростая (соответственно *нильпотентная*) *компонента эндоморфизма u' является сужением компоненты u_s* (соответственно u_n) *на подпространство W; полупростая* (соответственно *нильпотентная*) *компонента эндоморфизма u'' получается путем факторизации из u_s* (соответственно *из u_n*). *Кроме того, если эндоморфизм u_s диагонализируем, то u'_s и u''_s тоже диагонализируемы.*

В самом деле, пусть v' и w' — сужения эндоморфизмов u_s и u_n на W (подпространство W устойчиво относительно u_s и u_n ввиду предложения 8), v'' и w'' — эндоморфизмы пространства V/W, полученные соответственно из u_s и u_n путем факторизации. Ясно, что w' и w'' нильпотентны; по определению минимального многочлена эндоморфизма, минимальные многочлены сужений v' и v'' делят минимальный многочлен u_s; следовательно, v' и v'' полупросты (n° 2, предложение 5) и даже диагонализируемы, если диагонализируем эндоморфизм u_s (гл. VII, § 5, n° 4, предложение 10). Но $u' = v' + w'$, $u'' = v'' + w''$, и эндоморфизмы v' и w' (соответственно v'' и w'') коммутируют, так что доказываемое утверждение следует из предложения 8.

Предложение 10. *Предположим, что поле K совершенно. Пусть $\mathfrak{F}$ — такое множество попарно перестановочных эндоморфизмов пространства V, что корни минимальных многочленов всех $u \in \mathfrak{F}$ лежат в поле K. Тогда в пространстве V найдется базис, относительно которого всякий эндоморфизм $u \in \mathfrak{F}$ имеет треугольную матрицу, а матрица всякого u_s диагональна, и ее элементы совпадают с диагональными элементами матрицы эндоморфизма u.*

Пусть A — алгебра, порожденная множеством $\mathfrak{F}$ (и 1), и $(V_i)_{1 \leqslant i \leqslant m}$ — ряд Жордана — Гельдера A-модуля конечной длины V; A-модуль $W_i = V_i/V_{i+1}$ прост и имеет над K конечную размерность, алгебра A коммутативна; следовательно (§ 5, n° 2, предложение 9 и n° 4, предложение 12), кольцо гомотетий A_{W_i} является полем, расширением конечной степени поля K. По предположению, для любого $u \in \mathfrak{F}$ выполняется равенство $P(u) = 0$, где $P \in K[X]$ — многочлен, все корни которого лежат в K; следовательно, $P(u_{W_i}) = 0$, и поскольку u_{W_i} порождают поле A_{W_i}, то $A_{W_i} = K$; так как K-модуль W_i прост, то его размерность рав-

на 1. Далее, множество $\mathfrak{F}_s$ полупростых компонент эндоморфизмов $u \in \mathfrak{F}$ состоит из попарно перестановочных эндоморфизмов (следствие предложения 8) и, следовательно (n° 2, теорема 1 и предложение 4), полупросто; тогда в пространстве V_i подпространство V_{i+1} имеет дополнительную прямую D_i, устойчивую относительно всех элементов из $\mathfrak{F}_s$. Элементы $e_i \neq 0$, взятые из прямых D_i, образуют базис пространства V; относительно этого базиса все полупростые компоненты u_s эндоморфизмов $u \in \mathfrak{F}$ имеют диагональную матрицу; с другой стороны, нильпотентная гомотетия $(u_n)_{V_i}$ — нулевая; но $u_n(V_i) \subset V_i$, откуда ясно, что матрица эндоморфизма u_n относительно базиса (e_i) — треугольная и ее диагональные элементы равны нулю, что и заканчивает доказательство.

Упражнения. 1) Пусть u — эндоморфизм пространства $E = K^2$ и $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ — его матрица относительно канонического базиса пространства E. Показать, что если $(\alpha - \delta)^2 + 4\beta\gamma \neq 0$, то u абсолютно полупрост.

2) Пусть, в обозначениях упражнения 1, v — нильпотентный эндоморфизм пространства E, матрица которого относительно канонического базиса равна $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Привести пример абсолютно полупростого эндоморфизма u пространства E, для которого эндоморфизмы $u + v$ и uv абсолютно полупросты.

§ 10. Простые подкольца. Изоморфизмы простых колец

В этом параграфе остаются в силе соглашения, принятые в начале § 7.

1. *Теорема Сколема—Нетер*

Теорема 1 (Сколем — Нетер). *Пусть A — простая алгебра над полем K, центр которой совпадает с K, B — простая алгебра конечного ранга над полем K, f и g — K-изоморфизмы алгебры B на подалгебры алгебры A. Тогда существует такой внутренний автоморфизм ϑ алгебры A, что $g = \vartheta \circ f$.*

В самом деле, возьмем простой A-модуль S и отождествим A с его кольцом гомотетий (§ 5, n° 4, теорема 2). Коммутант модуля S есть тело D с центром K. По следствию 2 теоремы 2 § 7, n° 4,

алгебра $D \otimes_K B$ проста. Формулы

$$\left(\sum_i d_i \otimes b_i,\ s\right) \longrightarrow \sum_i d_i\,(f(b_i)\,s)$$

и

$$\left(\sum_i d_i \otimes b_i,\ s\right) \longrightarrow \sum_i d_i\,(g(b_i)\,s),$$

задающие на S внешние законы композиции, определяют на S две структуры $(D \otimes_K B)$-модуля; существование этих законов следует из того, что отображения

$$(d,\ b) \longrightarrow d\,(f(b)\,s) \quad \text{и} \quad (d,\ b) \longrightarrow d\,(g(b)\,s)$$

K-билинейны (гл. III, § 1, n° 2), и из формулы

$$\sum_i d_i\,(f(b_i)\left(\sum_j d'_j\,(f(b'_j)\,s)\right)) = \sum_i \sum_j d_i\,d'_j\,(f(b_i b'_j)\,s)$$

и аналогичной формулы, где f заменено на g, которые выполняются в силу того, что D — коммутант A-модуля S. Определенные таким образом два модуля имеют *одинаковую длину*: в самом деле, кольца D и $D \otimes_K B$ просты, и поэтому (§ 5, n° 6, формула (3)) эта длина в обоих случаях равна определителю $\dim_D S$, деленному на высоту $h(D \otimes_K B,\ D)$. Более того, эти модули изоморфны, поскольку кольцо $D \otimes_K B$ просто (§ 5, n° 2, предложение 8); иными словами, существует такой автоморфизм u абелевой группы S, что

$$(dg(b))\,s = (u\,df(b)\,u^{-1})\,s \tag{1}$$

для любых элементов $d \in D$, $b \in B$ и $s \in S$. Положив в этом равенстве $b = 1$, получаем, что $u \in \mathscr{L}_D(s) = A$. Положив в (1) $d = 1$, получаем $g(b) = uf(b)\,u^{-1}$, что и доказывает теорему.

Следствие. *Пусть A — полупростая алгебра конечного ранга над полем K, ϑ — ее внутренний автоморфизм, составляющий инвариантными элементы центра алгебры A. Тогда ϑ — внутренний автоморфизм.*

В самом деле, пусть A_i $(1 \leqslant i \leqslant n)$ — простые компоненты алгебры A (§ 5, n° 3) и e_i — единица алгебры A_i. Все элементы e_i лежат в центре алгебры A, и следовательно, $\vartheta(A_i) = \vartheta(e_i A) = e_i A = A_i$. Так как A — алгебра конечного ранга над K, то каждая A_i имеет конечный ранг над K и тем более над своим центром. По теореме 1 (примененной к каждой алгебре A_i, рас-

сматриваемой над своим центром) для всякого индекса i существует обратимый элемент $c_i \in A_i$ такой, что $\vartheta(x) = c_i x c_i^{-1}$ для всех $x \in A_i$. Взяв $c = \sum_{i=1}^{n} c_i$, будем иметь $\vartheta(x) = cxc^{-1}$ для всех $x \in A$.

Если A — тело, не имеющее конечного ранга над своим центром, то могут существовать и не внутренние автоморфизмы A, оставляющие инвариантными элементы центра тела A (упражнение 10).

Предложение 1. *Пусть V — векторное пространство над телом D.*

а) *Для любого автоморфизма σ тела D и любого биективного отображения g пространства V на себя, полулинейного относительно σ, отображение $u \to gug^{-1}$ является автоморфизмом кольца $\mathscr{L}_D(V)$.*

б) *Всякий автоморфизм кольца $\mathscr{L}_D(V)$ может быть получен этим способом.*

Первое утверждение очевидно. Пусть ϑ — автоморфизм кольца $\mathscr{L}_D(V)$. Формула $(a, x) \to \vartheta(a)\,x$ внешней композиции задает на V вторую структуру $\mathscr{L}_D(V)$-модуля, причем модуль V относительно обеих структур является простым и точным (§ 3, n° 1, пример 2). Заметим теперь, что кольцо $\mathscr{L}_D(V)$ обладает минимальными левыми идеалами (§ 3, n° 1, пример 2). Но тогда предложение 5 § 3, n° 1, показывает, что рассматриваемые на V структуры $\mathscr{L}_D(V)$-модулей изоморфны; иными словами, существует автоморфизм g абелевой группы V такой, что $\vartheta = gug^{-1}$ для любого $u \in \mathscr{L}_D(V)$. Но тело D (отождествленное с кольцом D_V гомотетий векторного пространства V) является коммутантом кольца $\mathscr{L}_D(V)$ (§ 1, n° 3, предложение 6), так что $gDg^{-1} = D$; отсюда следует, что сужение на D автоморфизма $u \to gug^{-1}$ кольца эндоморфизмов абелевой группы V будет автоморфизмом σ тела D. Тогда для любых $x \in V$ и $d \in D$ выполняется равенство $g(dx) = d^{\sigma} g(x)$, откуда и следует, что отображение g полулинейно относительно σ.

2. Простые подкольца простых колец

Теорема 2. *Пусть A — простое кольцо с центром K, B — его простое подкольцо, содержащее K. Если B конечного ранга над K, то:*

а) *коммутант B' кольца B в A — простое кольцо;*

б) *B совпадает со своим бикоммутантом в A*;

в) $[A : B'] = [B : K]$, $[A : B] = [B' : K]$ и $[A : K] = [B : K]\,[B' : K]$;

г) *B и B' линейно раздельны над своим общим центром* $B \cap B'$.

Пусть S — простой A-модуль, Ω — кольцо эндоморфизмов абелевой группы S, $D \subset \Omega$ — тело, коммутант модуля S; отождествим A с кольцом гомотетий $A_S \subset \Omega$ A-модуля S. Центр тела D совпадает с центром A, то есть равен K; поэтому (§ 7, n° 4, следствие 2 теоремы 2) алгебра $D \otimes_K B$ проста. Канонический гомоморфизм алгебры $D \otimes_K B$ в Ω (гл. III, § 3, n° 3) является, следовательно, изоморфизмом $D \otimes_K B$ на подкольцо, порожденное в Ω объединением $D \cup B$; это подкольцо представляет собой не что иное, как произведение DB абелевых подгрупп D и B в смысле § 6, n° 1. Тогда $[DB : D] = [D \otimes_K B : D] = [B : K]$ (гл. III, § 3, n° 3, теорема 1). Коммутант произведения DB в Ω является пересечением коммутанта A тела D в Ω и коммутанта кольца B в Ω и совпадает, следовательно, с коммутантом B' кольца B в A. С другой стороны, размерность $\dim_D S$ конечна (§ 5, n° 4, теорема 2), и, применяя предложение 16 § 5, n° 6, к DB-модулю S и простому подкольцу D кольца DB, убеждаемся, что кольцо B' просто и $[A : B'] = [DB : D] = [B : K]$. Следовательно, $[A : K] = [A : B']\,[B' : K] = [B : K]\,[B' : K]$. Но, с другой стороны, $[A : K] = [A : B]\,[B : K]$, так что $[A : B] = [B' : K]$, поскольку ранг $[B : K]$ конечен.

Бикоммутант DB-модуля S совпадает с DB (§ 5, n° 4, следствие 2 теоремы 2); следовательно, если некоторый элемент кольца A перестановочен со всеми элементами из B', то он входит в DB и перестановочен со всеми элементами из D; но тогда он перестановочен и со всеми элементами из B: это следует из того, что K — центр тела D и из изоморфности DB и $D \otimes_K B$ (§ 1, n° 2, предложение 3); отсюда следует утверждение б). Наконец, пусть $C = B \cap B'$ — общий центр подколец B и B'; поскольку $K \subset C$, то B' имеет над C конечный ранг. Следовательно (§ 7, n° 4, следствие 2 теоремы 2), алгебра $B \otimes_C B'$ проста и ее канонический гомоморфизм в A (гл. III, § 3, n° 3) является изоморфизмом на некоторую подалгебру в A, откуда следует утверждение г) (гл. III, § 3, n° 3, теорема 1).

Следствие. *Если центр кольца B равен K, то $A = BB'$ и кольцо A изоморфно $B \otimes_K B'$.*

В самом деле, по теореме 2г) BB' изоморфно $B \otimes_K B'$, то есть $[BB' : B'] = [B : K] = [A : B'] < +\infty$, что доказывает равенство $A = BB'$.

Пусть A — алгебра над полем K, M — A-модуль, B — подалгебра в A, содержащая ее единицу, B' — коммутант B в A; для любого $b' \in B'$ гомотетия b'_M модуля M принадлежит $\mathscr{L}_B(M)$ и коммутирует со всеми элементами $\mathscr{L}_A(M) \subset \mathscr{L}_B(M)$. Следовательно, имеется *канонический гомоморфизм* φ K-алгебры $\mathscr{L}_A(M) \otimes_K B'$ в K-алгебру $\mathscr{L}_B(M)$ такой, что $\varphi(u \otimes b') = ub'_M$ (гл. III, § 3, n° 3).

Предложение 2. *Пусть A — простое кольцо с центром K, и $M \neq \{0\}$ — A-модуль конечной длины; пусть B — простое подкольцо в A, содержащее K, и B' — его коммутант в K. Если алгебра A имеет над K конечный ранг, то канонический гомоморфизм K-алгебры $\mathscr{L}_A(M) \otimes_K B'$ в K-алгебру $\mathscr{L}_B(M)$ биективен.*

Так как A — алгебра конечного ранга над K, то модуль M имеет над K конечную размерность. Кольцо A не имеет двусторонних идеалов, отличных от $\{0\}$ и A, и отождествляется поэтому с кольцом гомотетий A_M; применив теорему 2а) к простой подалгебре A простой алгебры $\mathscr{L}_K(M)$ с центром K, получим, что алгебра $\mathscr{L}_A(M)$ проста и ее центр равен K. Алгебра B' проста по теореме 2а); следовательно, алгебра $\mathscr{L}_A(M) \otimes_K B'$ проста (§ 7, n° 4, следствие 2 теоремы 2) и канонический гомоморфизм этой алгебры в $\mathscr{L}_B(M)$ инъективен; пусть C — простая подалгебра в $\mathscr{L}_K(M)$, образе алгебры $\mathscr{L}_A(M) \otimes_K B'$ при этом гомоморфизме. Для доказательства равенства $C = \mathscr{L}_B(M)$ найдем коммутант C' подалгебры C в $\mathscr{L}_K(M)$. Коммутант $\mathscr{L}_A(M)$ в $\mathscr{L}_K(M)$ равен A (теорема 2б)); так как коммутант кольца B' в A есть B (теорема 2б)), то $C' = B$. Но C совпадает со своим бикоммутантом в простой алгебре $\mathscr{L}_K(M)$ (теорема 2б)), что и доказывает нужное равенство.

Следствие 1. *Пусть D — тело конечного ранга над своим центром K, $V \neq \{0\}$ — конечномерное векторное пространство над K. Канонический гомоморфизм K-алгебры $\mathscr{L}_D(V) \otimes_K D$ в K-алгебру $\mathscr{L}_K(V)$ биективен* (см. гл. III, § 3, n° 2, пример 11).

Это следствие является частным случаем предложения 2 при $A = D$, $B = K$, $M = V$.

Следствие 2. *Пусть A — простая алгебра конечного ранга m над своим центром K. Отождествим A и A^0 с подалгебрами в $\mathscr{L}_K(A)$, состоящими соответственно из левых и правых умножений алгебры A* (§ 1, n° 2); *канонический гомоморфизм K-алгебры $A^0 \otimes_K A$ в K-алгебру $\mathscr{L}_K(A)$ (изоморфную алгебре матриц $M_m(K)$) биективен.*

Так как $\mathscr{L}_A(M)$ является в условиях следствия кольцом правых умножений алгебры A (§ 1, n° 2, предложение 4), то утверждение получается как частный случай предложения 2 при $M = A_s$, $B = K$.

3. Подполя простых колец

Предложение 3. *Пусть A — простое кольцо с центром K и ранг A над K конечен. Для любого подполя L кольца A, содержащего K, следующие условия эквивалентны:*

а) *L совпадает со своим коммутантом в A;*

б) *L — максимальное коммутативное подкольцо в A;*

в) $[A : K] = [L : K]^2$.

Эквивалентность утверждений а) и б) очевидна. Эквивалентность а) и в) следует из теоремы 2в), n° 2.

В кольце A не всегда существует подполе L, удовлетворяющее условиям предложения 3: достаточно рассмотреть кольцо матриц $M_n(\Omega)$ над алгебраически замкнутым полем, $n > 1$.

Следствие. *Пусть D — тело конечного ранга над своим центром K, и L — подполе в D, содержащее K. Для того чтобы L было максимальным подполем в D, необходимо и достаточно, чтобы выполнялось равенство $[D : K] = [L : K]^2$.*

В самом деле, если A — коммутативное подкольцо в D, содержащее K, то A — подполе в D (гл. V, § 2, n° 1, предложение 1). Следовательно, максимальные подполя в D совпадают с его максимальными коммутативными подкольцами.

Таким образом, все максимальные подполя тела D являются расширениями поля K одной и той же степени. В то же время эти расширения не всегда изоморфны (§ 11, упражнение 4 и § 12, упражнение 9).

Лемма 1. *Пусть D — тело с центром K, D отлично от K и всякий его элемент алгебраичен над K. Тогда D содержит сепарабельное коммутативное расширение поля K степени > 1.*

Пусть $z \in D$ и $z \overline{\in} K$. Так как элемент z алгебраичен над K, то подалгебра $K(z) = K[z]$ тела D, порожденная K и z, является алгебраическим расширением поля K конечной степени > 1. Если элемент z не радикален над K, то $K(z)$ содержит сепарабельное расширение поля K степени >1 (гл. V, § 8, n° 4, следствие предложения 7). Пусть z радикален над K; так как $z \overline{\in} K$, то характеристика p поля $K > 0$ и существует целое число $e \geqslant 0$ такое, что $u = z^{p^e} \overline{\in} K$, но $u^p \in K$. Пусть σ — автоморфизм $x \to uxu^{-1}$ векторного K-пространства D. Имеем $\sigma^p = 1$ (тождественный автоморфизм пространства D), следовательно, $(\sigma - 1)^p = 0$, а $\sigma - 1 \neq 0$, поскольку $u \overline{\in} K$. Пусть r — наибольшее число для которого $(\sigma - 1)^r \neq 0$, и y — элемент тела D такой, что $(\sigma - 1)^r(y) \neq 0$; положим $a = (\sigma - 1)^{r-1}(y)$, $b = (\sigma - 1)(a)$, $c = a^{-1}b$. По определению r, $\sigma(b) = b$ и $\sigma(c) = b^{-1}\sigma(a) = b^{-1}(b + a) = 1 + c \neq c$. Таким образом, коммутативное расширение $K(c)$ поля K устойчиво относительно σ и сужение автоморфизма σ на $K(c)$ отлично от тождественного автоморфизма. Следовательно (гл. V, § 8, n° 4, предложение 8), наибольшее сепарабельное расширение поля K, содержащееся в $K(c)$, имеет степень > 1, что и доказывает лемму.

Предложение 4. *Пусть D — тело конечного ранга над своим центром K. Тогда в D имеется максимальное подполе, являющееся сепарабельным расширением поля K.*

Положим $[D : K] = n^2$ и будем доказывать предложение индукцией по n. При $n = 1$ оно тривиально. При $n > 1$, по лемме 1, существует отличное от K сепарабельное коммутативное расширение $L \subset D$ поля K. Коммутант L' подполя L в D является подтелом в D, и его центр, по теореме 2б), равен L. Имеем $[L' : L] < n^2$, и, по предположению индукции, L' содержит максимальное подполе M, являющееся сепарабельным расширением поля L. Всякое подполе тела D, содержащее M, содержит K, следовательно, содержится в L' и равно M. Таким образом, M — максимальное подполе тела D. Так как M сепарабельно над L и L сепарабельно над K, то M сепарабельно над K (гл. VII, § 7, n° 4, предложение 7).

4. Группа Брауэра

Пусть K — поле. Напомним (§ 5, n° 4, следствие 2 предложения 12), что всякая простая алгебра A с центром K и *конечного* ранга над K изоморфна кольцу матриц $\boldsymbol{M}_r(D)$ над некоторым телом D с центром K и конечного ранга над K; кроме того, тело D K-изоморфно телу, противоположному телу эндоморфизмов любого минимального идеала кольца A (§ 5, n° 4, теорема 2).

Определение 1. *Простые алгебры A и B с центром K конечного ранга над K называются подобными, если существуют тело D с центром K и целые числа $r \geqslant 0$, $s \geqslant 0$ такие, что A и B изоморфны соответственно $\boldsymbol{M}_r(D)$ и $\boldsymbol{M}_s(D)$.*

Таким образом, все кольца матриц $\boldsymbol{M}_n(D)$ над телом D с центром K и конечного ранга над K *подобны* D. Две подобные простые алгебры с центром K, имеющие одинаковый конечный ранг над K, *изоморфны*; два подобных тела с центром K и конечного ранга над K *изоморфны*.

Если A и B — простые алгебры с центром K конечного ранга над K, то алгебра $A \otimes B$ проста (§ 7, n° 4, следствие 2 теоремы 2), ее центр равен K (§ 1, n° 2, следствие предложения 3) и ее ранг над K конечен. Кроме того,

Предложение 5. *Пусть A, A_1, B, B_1 — простые алгебры конечного ранга над своим центром K, A подобна A_1 и B подобна B_1. Тогда $A \otimes B$ подобна $A_1 \otimes B_1$.*

В самом деле, алгебра A (соответственно A_1) изоморфна алгебре вида $\boldsymbol{M}_p(D)$ (соответственно $\boldsymbol{M}_r(D)$), алгебра B (соответственно B_1) изоморфна алгебре вида $\boldsymbol{M}_q(E)$ (соответственно $\boldsymbol{M}_s(E)$), где D и E — тела конечного ранга над своим центром K. Алгебра $D \otimes E$ проста, ее центр равен K, и следовательно, она изоморфна алгебре $\boldsymbol{M}_h(L)$, где L — тело конечного ранга над своим центром K. Известно, что для всякой алгебры C над полем K-алгебра $\boldsymbol{M}_n(C)$ изоморфна $C \otimes \boldsymbol{M}_n(K)$ (гл. III, § 3, n° 2) и что тензорное произведение $\boldsymbol{M}_m(K) \otimes \boldsymbol{M}_n(K)$ изоморфно $\boldsymbol{M}_{mn}(K)$ (гл. III, § 3, n° 2); отсюда следует, что алгебра $A \otimes B$ изоморфна $\boldsymbol{M}_{hpq}(L)$, а $A_1 \otimes B_1$ изоморфна $\boldsymbol{M}_{hrs}(L)$, что и доказывает предложение.

Обозначим через $Sm_K(X, Y)$ отношение

«K — поле, и X, Y — подобные простые алгебры с центром K конечного ранга над K».

Ясно, что это есть отношение эквивалентности между X и Y. Если X и Y — подобные простые алгебры (с центром K конечного ранга над K), то истинно отношение $(\forall Z)\,(Sm_K(X, Z) \Rightarrow Sm_K(Y, Z))$. Но схема S7 (Теор. мн., гл. I, § 5, n° 1) дает следующую аксиому:

$$((\forall Z)\,(Sm_K(X, Z) \Rightarrow (Sm_K(Y, Z))) \Rightarrow (\tau_Z(Sm_K(X, Z)) = \tau_Z(Sm_K(Y, Z))).$$

Следовательно, если X и Y — подобные простые алгебры конечного ранга над своим центром K, то

$$\tau_Z(Sm_K(X, Z)) = \tau_Z(Sm_K(Y, Z)).$$

Для любой простой алгебры конечного ранга над своим центром K $\tau_Z(Sm_K(A, Z))$ называется *классом алгебры* A; говорят также, что A — алгебра класса $\tau_Z(Sm_K(A, Z))$. Так как отношение $Sm_K(A, A)$ истинно, то класс алгебры A является простой алгеброй, подобной A. Таким образом, для подобия двух простых алгебр конечного ранга над своим центром K необходимо и достаточно, чтобы они были одного класса.

Теперь мы докажем, что отношение

«α есть класс простых алгебр с центром K конечного ранга над K»

является *коллективизирующим* по α (Теор. мн. гл. II, § 1, n° 4). Пусть $\mathscr{A}_n$, $n \geqslant 1$,— множество подалгебр K-алгебры $\mathscr{L}_K(K^n)$, содержащих единицу этой алгебры, и $\mathscr{A}$ — объединение семейства $(\mathscr{A}_n)_{n \geqslant 1}$. Всякая алгебра A ранга n над полем K изоморфна алгебре левых умножений кольца A (§ 1, n° 2); так как векторное пространство A изоморфно K^n, то алгебра A изоморфна некоторой алгебре, принадлежащей $\mathscr{A}_n$. Пусть тогда $\mathscr{S}$ — множество простых алгебр с центром K, принадлежащих $\mathscr{A}$, и $\mathscr{B}(K)$ — множество объектов вида $\tau_Z(Sm_K(X, Z))$ для $X \in \mathscr{S}$ (Теор. мн., гл. II, § 1, n° 6). Ясно, что для любого класса α простых алгебр конечного ранга над своим центром K имеем $\alpha \in \mathscr{B}(K)$; $\mathscr{B}(K)$ называется *множеством классов простых алгебр конечного ранга над своим центром* K.

Определим теперь на множестве $\mathscr{B}(K)$ структуру *абелевой группы*. Пусть $\alpha, \beta \in \mathscr{B}(K)$; обозначим через $\alpha\beta$ класс простой

алгебры $\alpha \otimes \beta$; ввиду изоморфности произведений $\alpha \otimes \beta$ и $\beta \otimes \alpha$ определенный таким образом закон композиции *коммутативен*. Для доказательства его ассоциативности заметим, что класс $(\alpha\beta)\gamma$ подобен $(\alpha\beta) \otimes \gamma$, а класс $\alpha(\beta\gamma)$ подобен $\alpha \otimes (\beta\gamma)$; тогда по предложению 5 $(\alpha\beta)\gamma$ подобен $(\alpha \otimes \beta) \otimes \gamma$, а $\alpha(\beta\gamma)$ подобен $\alpha \otimes (\beta \otimes \gamma)$; таким образом, наше утверждение следует из того, что $(\alpha \otimes \beta) \otimes \gamma$ и $\alpha \otimes (\beta \otimes \gamma)$ изоморфны. Теперь покажем, что класс ε поля K является *нейтральным элементом* в $\mathscr{B}(K)$; в самом деле, ε изоморфен некоторой алгебре $M_n(K)$; для любого класса $\alpha \in \mathscr{B}(K)$, изоморфного некоторой алгебре вида $D \otimes M_p(K)$ (где D — тело с центром K), класс $\varepsilon\alpha$ подобен $D \otimes M_{np}(K)$ и, следовательно, подобен α. Наконец (n° 2, следствие 2 предложения 2), для любого $\alpha \in \mathscr{B}(K)$ класс $\alpha \otimes \alpha^0$ изоморфен алгебре матриц $M_n(K)$, то есть $\alpha\alpha^0 = \varepsilon$, откуда следует, что α^0 — *обратный элемент* к α в $\mathscr{B}(K)$.

Определение 2. *Пусть K — поле. Группой Брауэра поля K называется множество $\mathscr{B}(K)$ классов простых алгебр с центром K конечного ранга над K, наделенное законом композиции $(\alpha, \beta) \to \alpha\beta$, где $\alpha\beta$ — класс простой алгебры $\alpha \otimes \beta$.*

Примеры. 1) Если поле K алгебраически замкнуто, то всякая простая алгебра конечного ранга над полем K изоморфна алгебре матриц $M_n(K)$ (§ 5, n° 4, следствие 3 предложения 12). Следовательно, группа Брауэра в этом случае сводится к нейтральному элементу.

*2) В § 11, n° 1, мы увидим, что если поле K конечно, то всякое тело конечного ранга над K коммутативно; следовательно, простые алгебры конечного ранга над своим центром K также изоморфны алгебрам матриц $M_n(K)$ и группа $\mathscr{B}(K)$ сводится к нейтральному элементу.

3) В § 11, n° 2, мы увидим, что группа Брауэра максимального упорядоченного поля является *циклической группой порядка* 2.

4) Можно показать, что если K — локально компактное нормированное тело, абсолютное значение которого валюативно, то группа Брауэра $\mathscr{B}(K)$ изоморфна $\boldsymbol{Q}/\boldsymbol{Z}$ («рациональные числа по mod 1»).

5. *Нейтрализующие поля*

Пусть K — поле, L — его расширение. Для любой алгебры A с центром K и конечного ранга над K алгебра $A_{(L)}$, получаемая расширением поля скаляров до L, представляет собой не что иное, как тензорное произведение $A \otimes L$, рассматриваемое как

алгебра над L (гл. III, § 3, n° 4); следовательно, эта алгебра *проста*, ее *центр равен* L (§ 7, n° 4, следствие 2 теоремы 2) и ее ранг над L равен рангу A над K. Заметим теперь, что если A и B — алгебры над полем L, то L-алгебра $A_{(L)} \otimes_L B_{(L)}$ канонически изоморфна $(A \otimes B)_{(L)}$: в самом деле, по свойствам тензорных произведений (гл. III, §§ 1, 3 и приложение II) алгебры $A \otimes B \otimes L$, $A \otimes (L \otimes_L L) \otimes B$, $A \otimes (L \otimes_L (L \otimes B))$ и $(A \otimes L) \otimes_L (B \otimes L)$ канонически отождествимы.

Пусть D — тело конечного ранга над своим центром K. Применяя предыдущее замечание к тензорному произведению $D \otimes \boldsymbol{M}_n(K)$, изоморфному $\boldsymbol{M}_n(D)$, убеждаемся, что алгебра $(\boldsymbol{M}_n(D))_{(L)}$ изоморфна $(D \otimes L) \otimes_L \boldsymbol{M}_n(L)$; отсюда можно заключить, что в случае, когда A и B — *подобные* простые алгебры конечного ранга над своим центром K, алгебры $A_{(L)}$ и $B_{(L)}$ над полем L *подобны*. Для любого класса $\alpha \in \mathscr{B}(K)$ через α_L обозначим класс простой алгебры $\alpha_{(L)}$.

Предложение 6. *Пусть L — расширение поля K. Тогда отображение $\alpha \to \alpha_{(L)}$ является гомоморфизмом группы $\mathscr{B}(K)$ в группу $\mathscr{B}(L)$.*

В самом деле, пусть $\alpha \in \mathscr{B}(K)$, $\beta \in \mathscr{B}(K)$; тогда $(\alpha\beta)_{(L)}$, по определению, подобна $(\alpha \otimes \beta)_{(L)}$, т. е. $\alpha_{(L)} \otimes_L \beta_{(L)}$, и, следовательно, подобна $\alpha_L\beta_L$; таким образом, по определению, $(\alpha\beta)_L = \alpha_L\beta_L$.

Ядро $\mathscr{N}_{L,K}$ гомоморфизма $\alpha \to \alpha_L$ является в $\mathscr{B}(K)$ подгруппой и состоит из таких классов α, что для любой простой алгебры A класса α алгебра $A_{(L)}$ изоморфна алгебре матриц $\boldsymbol{M}_n(L)$; если класс простой алгебры A конечного ранга над своим центром K принадлежит $\mathscr{N}_{L,K}$, то говорят, что алгебра A *нейтрализуется* расширением L поля K, а расширение называют *нейтрализующим* относительно A (или, допуская вольность речи, *нейтрализующим полем* алгебры A). Если расширения E и F поля K связаны включением $E \subset F$, то из изоморфности алгебр $(\alpha_{(E)})_{(F)}$ и $\alpha_{(F)}$ (гл. III, § 3, n° 4) следует, что $(\alpha_E)_F = \alpha_F$ для любого $\alpha \in \mathscr{B}(K)$; отсюда $\mathscr{N}_{E,K} \subset \mathscr{N}_{F,K}$.

Замечание. Пусть D — простая алгебра конечного ранга над своим центром K. Следующие три свойства эквивалентны:

а) L — нейтрализующее поле алгебры A;

б) L-алгебра $A_{(L)}$ изоморфна алгебре матриц над некоторым полем;

в) коммутант всякого простого модуля S над $A_{(L)}$ совпадает с полем гомотетий L_S.

В самом деле, эквивалентность свойств а) и б) следует из того, что центр алгебры $A_{(L)}$ равен L; эквивалентность свойств а) и в) следует из того, что алгебра $A_{(L)}$, будучи простой, изоморфна бикоммутанту простого $A_{(L)}$-модуля S (§ 5, n° 4, теорема 2).

Предложение 7. *Пусть K — поле, L — его расширение конечной степени, A — простая алгебра конечного ранга над своим центром K. Следующие два свойства эквивалентны:*

а) *L — нейтрализующее поле алгебры A;*

б) *существует алгебра B, подобная A и такая, что поле L K-изоморфно максимальному коммутативному подкольцу алгебры B.*

Докажем, что а) влечет б). По предположению, можно считать, что алгебра $A_{(L)}$ отождествлена с алгеброй $\mathscr{L}_L(V)$ эндоморфизмов векторного пространства V конечной размерности над полем L. A-модуль V имеет конечную длину, и поле L (отождествленное с полем гомотетий пространства V) является коммутантом $A_{(L)}$-модуля V; поэтому коммутант C A-модуля V является простым кольцом, содержащим L, и $[C, L] = [A_{(L)} : A] = [L : K]$ (§ 5, n° 6, предложение 16); кроме того, общий центр A и C равен K, так что, ввиду равенства $[C, K] = [C, K]^2$, L будет в алгебре C максимальным коммутативным подкольцом (n° 3, предложение 3). Наконец, если D — тело эндоморфизмов простого A-модуля, то D^0 изоморфно телу эндоморфизмов простого C-модуля (§ 4, n° 4, предложение 4); это показывает, что классы алгебр A и C обратны друг другу в $\mathscr{B}(K)$; следовательно, алгебра $B = C^0$ подобна A, и поле L, очевидно, является ее максимальным коммутативным подкольцом.

Докажем, что, обратно, б) влечет а). Пусть поле L — максимальное коммутативное подкольцо алгебры B; отождествим B с кольцом $\mathscr{L}_D(V)$ эндоморфизмов векторного пространства V, конечномерного над телом D; тогда D будет коммутантом B-модуля V. С другой стороны, коммутант поля L в B есть само поле L; из предложения 2 n° 2 следует тогда, что алгебра $D_{(L)}$ изоморфна алгебре $\mathscr{L}_L(V)$, то есть L — нейтрализующее поле алгебры D; так как классы алгебр B и D обратны друг другу, то

L будет также нейтрализующим полем для любой алгебры, подобной B.

Следствие 1. *Пусть D — тело конечного ранга над своим центром K, и $[D : K] = r^2$. Если нейтрализующее поле L тела D имеет конечную степень над K, то $[L : K]$ кратно r.*

В самом деле, по предложению 7 существует алгебра A, подобная D, в которой поле L является максимальным коммутативным подкольцом; но алгебра A изоморфна некоторой алгебре матриц $\boldsymbol{M}_n(D)$, так что $[A : K] = n^2r^2$, откуда $[L : K] = nr$ (n° 3, предложение 3).

Следствие 2. *Пусть D — тело конечного ранга над своим центром K. Всякое максимальное подполе тела D является нейтрализующим полем для D.*

Не следует думать, что всякое нейтрализующее поле тела D содержит подполе, изоморфное некоторому его максимальному подполю (см. § 12, упражнение 12).

Следствие 3. *Всякая простая алгебра A конечного ранга над своим центром K обладает нейтрализующим полем, являющимся расширением Галуа конечной степени поля K.*

В самом деле, пусть D — тело, подобное A; по предложению 4 n° 3 D содержит максимальное подполе L, являющееся сепарабельным расширением поля K. Из предложения 7 следует, что расширение Галуа N поля K, порожденное полем L (в алгебраическом замыкании поля K), будет нейтрализующим полем алгебры A.

Мы видим, таким образом, что группа $B(K)$ является объединением подгрупп $\mathscr{G}_{N,K}$, соответствующих расширениям Галуа N конечной степени поля K. Более глубокое изучение группы Брауэра состоит именно в описании структуры групп $\mathscr{G}_{N,K}$ с помощью теории «скрещенных произведений».

Упражнения. 1) Пусть A — простая алгебра $\boldsymbol{M}_5(K)$ (K — поле), B — ее подалгебра, состоящая из матриц вида

$$\begin{pmatrix} x & 0 & 0 \\ 0 & Y & 0 \\ 0 & 0 & Y \end{pmatrix},$$

C — подалгебра, состоящая из матриц вида

$$\begin{pmatrix} x & 0 & 0 & 0 \\ 0 & x & 0 & 0 \\ 0 & 0 & x & 0 \\ 0 & 0 & 0 & Y \end{pmatrix},$$

где x пробегает K, а Y — алгебру $M_2(K)$. Показать, что B и C — полупростые алгебры, содержащие центр алгебры A, и существует K-изоморфизм f алгебры B на C, оставляющий инвариантными элементы центра алгебры A, но не существует внутреннего автоморфизма алгебры A, продолжающего f (заметить, что такой автоморфизм не может переводить простую компоненту алгебры B в простую компоненту алгебры C).

*2) а) Пусть A — алгебра над полем K, B — ее простая подалгебра, имеющая конечный ранг над своим центром K, B' — коммутант подалгебры B и A. Показать, что канонический гомоморфизм алгебры $B \otimes_K B'$ в A является биекцией на A. (Заметить сначала, что B и B' линейно раздельны над K (§ 7, упражнение 6г)); с другой стороны, алгебру A можно рассматривать как $(B \otimes B^0)$-модуль (§ 7, упражнение 1); применяя следствие 2 предложения 2, показать, что A является прямой суммой $(B \otimes B^0)$-модулей M_α, изоморфных B; заметить, наконец, что $\varphi_\alpha(1) \in B'$, где φ_α — $(B \otimes B^0)$-изоморфизм модуля B на M_α.)

б) Обратно, пусть B — алгебра над полем K такая, что для всякой алгебры A, содержащей B и имеющей с ней общую единицу, канонический гомоморфизм алгебры $B \otimes_K B'$ в A (где B' — коммутант B в A) биективен. Показать, что алгебра B проста, ее центр равен K и ее ранг над K конечен. (Отождествив B с его кольцом левых умножений $\mathscr{H}_L$, применить предположение к случаю $A = \mathscr{L}_K(B)$; пользуясь предложением 4 § 1, п° 2, вывести отсюда сначала, что алгебра B квазипроста (§ 5, упражнение 5) и что центр B есть K; отсюда, пользуясь упражнением 6 § 7, вывести, что алгебра $\mathscr{L}_K(B)$ проста и имеет конечный ранг над K.)

*3) Пусть V — левое векторное пространство над телом D с центром Z, Ω — кольцо эндоморфизмов абелевой группы V; отождествим D с подкольцом $D_V \subset \Omega$ гомотетий пространства V. Пусть Γ — группа автоморфизмов тела D, Δ — группа его внутренних автоморфизмов, откуда следует, что Δ изоморфна D^*/Z^*, для любого автоморфизма $\sigma \in \Gamma$ через $\bar{\sigma}$ обозначим класс $\sigma \pmod{\Delta}$, через $C(\bar{\sigma})$ — множество полулинейных отображений пространства V в себя, соответствующих автоморфизмам тела D из класса $\bar{\sigma}$; в частности, $C(\bar{1})$ состоит из элементов вида $\lambda u = u\lambda$, где $\lambda \in D$ и $u \in \mathscr{L}_D(V) = A$.

а) Пусть M — множество полулинейных отображений пространства V в себя, F — левое векторное подпространство над телом D,

порожденное в Ω множеством M (совпадающее с правым векторным подпространством над телом D, порожденным M). Пусть $F(\bar{\sigma})$, где $\bar{\sigma} \in \Gamma/\Delta$,— подпространство, порожденное в F элементами $u \in M$, лежащими в $C(\bar{\sigma})$; тогда F является прямой суммой подпространств $F(\bar{\sigma})$. Кроме того, всякое множество N полулинейных отображений пространства V в себя, входящее целиком в некоторый класс $C(\bar{\sigma})$ и свободное над Z, свободно также (слева и справа) над D. (Доказывать одновременно оба утверждения, рассматривая для этого первичные соотношения (гл. II, § 5, n° 4) между полулинейными отображениями с коэффициентами из тела D.)

б) Показать, что всякое подмножество $H \subset F$, являющееся одновременно левым и правым векторным пространством над D, порождается полулинейными отображениями пространства V в себя, входящими в подпространства $F(\bar{\sigma})$. (Рассматривая F и H как левые векторные D-пространства, выбрать в F базис, составленный из элементов $M \cap C(\bar{\sigma})$, а в H взять элементы, первичные относительно этого базиса (гл. II, § 5, n° 2).)

*4) Пусть V — векторное пространство над телом D с центром Z, Ω — кольцо эндоморфизмов абелевой группы V, A — кольцо $\mathscr{L}_D(V)$, коммутант пространства V. Пусть s — автоморфизм кольца A; множество таких элементов $v \in \Omega$, что $s(a) = vav^{-1}$ для любого $a \in A$, образует в Ω подпространство (левое и правое) $Du = uD$, где u — некоторая полулинейная биекция пространства V на себя. Пусть $U(G)$, где G — некоторая группа автоморфизмов кольца A,— векторное подпространство (левое и правое) над телом D, порожденное в Ω полулинейными биекциями пространства V, соответствующими элементам группы G, коммутант $I(G)$ этого подпространства в Ω является в A подкольцом, состоящим из элементов, инвариантных относительно G. Пусть G_0 — подгруппа в G, состоящая из *внутренних* автоморфизмов кольца A, $S(G)$ — векторное пространство *над* полем Z, порожденное обратимыми элементами кольца A, соответствующими элементам группы G_0; $S(G)$ является подкольцом в $\mathscr{L}_D(V)$, содержащим Z.

а) Пусть (c_α) — базис пространства $S(G)$ над Z, составленный из обратимых элементов кольца A, определяющих внутренние автоморфизмы из группы G_0; пусть (s_β) — система представителей классов группы G по mod G_0, и для каждого s_β пусть u_β — соответствующая ему полулинейная биекция пространства V. Показать, что элементы $c_\alpha u_\beta$ образуют базис (левый и правый) пространства $U(G)$ над телом D (использовать упражнение 3а)). В частности, размерность $[U(G) : D]$ конечна тогда и только тогда, когда конечны $(G : G_0)$ и $[S(G) : Z]$, и в этом случае $[U(G) : D] = (G : G_0)\,[S(G) : Z]$.

б) Показать, что $S(G) = U(G) \cap A$ и что пространство $U(G_0) = DS(G)$ канонически изоморфно $S(G) \otimes_Z D$ (воспользоваться упражнением 3а) § 10 и упражнением 19 § 7).

в) Элемент $v \in U(G)$ является полулинейным отображением пространства V в себя тогда и только тогда, когда он имеет вид $\lambda c u_\beta$, где $\lambda \in D$ и $c \in S(G)$ (использовать б) и упражнение 3а)).

г) Показать, что $I(G) \cap Z$ — поле и $I(G)$ и Z линейно раздельны над $I(G) \cap Z$ (рассмотреть первичное соотношение с коэффициентами из Z между элементами некоторого семейства из $I(G)$, свободного над $I(G) \cap Z$).

д) Показать, что если кольцо $S(G)$ просто и $S(G)$ и D имеют конечный ранг над Z, то кольцо $U(G)$ квазипросто (использовать б) и упражнение 3а), примененное к двустороннему идеалу кольца $U(G)$).

е) Пусть пространство V конечномерно над D, $U(G)$ имеет конечный ранг над D и кольцо $S(G)$ просто. Показать, что кольцо $I(G)$ просто и $[A : I(G)] = [S(G) : Z](G : G_0)$. Кроме того, $U(G)$ есть коммутант кольца $I(G)$ в Ω, а $S(G)$ — коммутант кольца $I(G)$ в A. Наконец, группа $\overline{G}$ автоморфизмов кольца A, оставляющих инвариантными элементы $I(G)$, состоит из автоморфизмов вида $a \to vav^{-1}$, где v пробегает множество обратимых элементов кольца $U(G)$ (воспользоваться упражнением 16 § 5, n° 6). Если $G_0 = G$, то $I(G)$ содержит Z в случае, когда ранг $[D : Z]$ конечен, верно обратное утверждение.

*5) Сохраняя обозначения упражнения 4, предположим, что размерность пространства V над телом D *конечна*. Подкольцо C называется *слабым подкольцом Галуа* кольца A, если его коммутант $C' \subset D$ в Ω порождается, как векторное D-пространство (левое или правое), полулинейными отображениями пространства V в себя (не обязательно биективными).

а) Показать, что если слабое подкольцо Галуа C полупросто, то V — полупростой модуль конечной длины над кольцом DC, порожденным в Ω подкольцами C и D. (Пусть N_i $(1 \leqslant i \leqslant s)$ — изотипные компоненты полупростого C-модуля V; каждая компонента N_i является DC-модулем конечной длины; пусть M — простой подмодуль этого DC-модуля. Показать, что для любого полулинейного отображения $v \in C'$ пространства V в себя $v(M)$ также является DC-модулем, и N_i содержится в сумме модулей $v(M)$, где v пробегает множество полулинейных отображений, содержащихся в C'; для этого использовать упражнение 7б) § 4; в заключение применить предложение 8 § 3, n° 3.)

б) Предположим, что слабое подкольцо Галуа C просто и его коммутант $C'_0 = A \cap C'$ в A — *простое* кольцо (см. упражнение 9); показать, что V — изотипный полупростой DC-модуль (заметить, что C'_0 является коммутантом подкольца DC в Ω, и применить предложение 5 § 4, n° 4). Вывести отсюда, что C' *порождается* (как векторное пространство над телом D) биективными полулинейными отображениями; в этом случае C называется *подкольцом Галуа* коль-

ца A. (Пусть $v \in C'$ — полулинейное отображение $\neq 0$ пространства V в себя, и $V = \sum_{i=1}^{n} M_i$ — разложение пространства V в прямую сумму изоморфных простых DC-модулей; можно считать, что $v(M_1) = N_1 \neq \{0\}$; тогда найдется разложение $V = \sum_{i=1}^{n} N_i$ пространства V на изоморфные простые DC-модули, один из которых есть N_1; вывести отсюда, что существует биективное полулинейное отображение w пространства V в себя, принадлежащее C', совпадающее с v на M_1 и такое, что $u = vw^{-1} \in C'_0$; в заключение воспользоваться следующей леммой: всякая квадратная матрица порядка n над телом D является суммой обратимых матриц порядка n; эту лемму можно доказать, заметив, что если матрица U нильпотентна, то матрица $1 - U$ обратима.)

* 6) Сохраняя обозначения упражнения 4, предположим, что размерность пространства V *конечна*. Некоторая группа G автоморфизмов кольца $A = \mathscr{L}_D(V)$ называется *группой Галуа*, если она удовлетворяет следующим условиям: 1° $(G : G_0)$ и $[S(G) : Z]$ конечны; 2° $S(G)$ — простое кольцо; 3° для любого обратимого элемента $c \in S(G)$ внутренний автоморфизм $a \to cac^{-1}$ принадлежит G_0.

а) Пусть $\mathscr{G}$ — множество подгрупп Галуа группы G. Показать, что отображение $H \to I(H)$ является убывающей биекцией множества $\mathscr{G}$ на множество простых подколец C кольца A, содержащих $I(G)$, у которых коммутант C'_0 в A прост. (Для доказательства инъективности этого отображения использовать упражнение 4е). Для доказательства сюръективности сначала с помощью упражнений 3б) и 5 установить, что кольцо C, удовлетворяющее указанным условиям, будет *кольцом Галуа* (упражнение 5); показать, наконец, что если H — группа автоморфизмов кольца A, оставляющих инвариантными элементы C, то $C = I(H)$ (использовать упражнение 16 § 5, n° 6) и H — группа Галуа.)

б) Пусть C_1, C_2 — простые подкольца в A, содержащие $I(G)$, и их коммутанты в A просты. Показать, что для любого изоморфизма φ кольца C_1 на C_2, оставляющего инвариантными элементы $I(G)$, существует элемент из группы G, совпадающий на C_1 с φ. (Используя равенство $h(C_1, I(G)) = h(C_2, I(G))$, показать сначала, что длина V как C_1-модуля совпадает с его длиной как C_2-модуля. Вывести отсюда, что длина его как DC_1-модуля совпадает с его длиной как DC_2-модуля; для этого заметить, что множество W таких элементов $f \in \Omega$, что $f(c_1 x) = \varphi(c_1) f(x)$ для любых $c_1 \in C$ и $x \in V$, не сводится к 0 и к нему можно применить результат упражнения 3б); если $w \neq 0$ — полулинейное отображение пространства V в себя, принадлежащее W, и M_1 — простой подмодуль DC_1-модуля V такой, что $w(M_1) = N_1 = \{0\}$, то сужение отображения w на M_1 является

биекцией на N_1 и длина C_1-модуля M_1 равна длине C_2-модуля N_1 (использовать упражнение 5б)). В заключение, рассуждая, как в упражнении 5б), показать, что существует биективное полулинейное отображение $v \in W$, совпадающее на M_1 с w.)

в) Рассмотреть следующие частные случаи результатов а) и б): 1° $G = G_0$ (см. n° 2, теорема 2); 2° $G_0 = \{1\}$; показать, что всякая конечная группа автоморфизмов кольца G, удовлетворяющая этому условию, будет группой Галуа и коммутант в A любого его простого подкольца, содержащего $I(G)$, равен Z; 3° размерность пространства V равна 1, откуда следует, что A есть тело, изоморфное D^0; $I(G)$ — тело, и коммутант в A любого его подтела, содержащего $I(G)$, есть тело. Разобрать частный случай, когда D — поле (см. гл. V, § 10).

*7) Пусть D — тело с центром Z, отождествленное с кольцом эндоморфизмов $\mathscr{L}_{D^0}(D_r)$ (§ 1, n° 2), и D^0 отождествлено с кольцом гомотетий модуля D_r. Пусть G — некоторая группа Галуа (упражнение 6) автоморфизмов тела D; положим, в обозначениях упражнения 6, $E = I(G)$, $E' = S(G)$; E и E' являются в D подтелами, и E' — коммутант E в D. Тогда группу G можно отождествить с подмножеством таких элементов $u \in U(G)$, что $u(1) = 1$. E^0 отождествляется с подтелом в D^0, состоящим из гомотетий $\lambda_r : \xi \to \xi\lambda$ модуля D_r, где $\lambda \in E$; выполняется равенство $[D^0 : E^0] = [D : E]$.

а) Обозначим через B подкольцо, порожденное в Ω множествами G и E^0; это будет векторное пространство над E^0. Показать, что $[B : E^0] = [D, E]$ тогда и только тогда, когда либо $E' = Z$ (иными словами, $G_0 = \{1\}$), либо $E' \subset E$. (Заметить, что в обозначениях упражнения 4а) можно считать, что $u_\beta \in G$; тогда в пространстве $U(G)$ над D^0 имеется базис, состоящий из элементов $(c_\alpha^{-1})_r c_\alpha u_\beta$, принадлежащих G; можно считать, что один из элементов c_α равен 1. Для доказательства необходимости условия заметить, что если оно не выполнено, то один из элементов c_α не принадлежит E; выразив затем элемент $(1 + c_\alpha)_r^{-1}(1 + c_\alpha)$ кольца B через указанный базис пространства $U(G)$, показать, что этот базис не может быть базисом B над E^0.)

б) Предположим, что $E' = Z$ или $E' \subset E$. Показать, что $U(G)$ является B-модулем с базисом из $n = [D : E]$ элементов. С другой стороны, $U(G)$ отождествляется с $\mathscr{L}_E(D_E)$, где D_E есть тело D, рассматриваемое как векторное E-пространство (упражнение 4е)); вывести отсюда, что $U(G)$ как $U(G)$-модуль является прямой суммой n подмодулей, изоморфных D, рассматриваемому как $U(G)$-модуль (§ 1, упражнение 8в)), и, следовательно, $U(G)$ как B-модуль также является прямой суммой n подмодулей, изоморфных D (рассматриваемому как B-модуль). В заключение доказать, что B-модуль D *моногенен* (см. § 2, упражнение 2), иными словами, пространство D над телом E имеет *нормальный базис*, состоящий из образов некоторого элемента D при некоторых автоморфизмах группы G.

*8) Сохраняя обозначения и предположения упражнения 7, будем считать, что поле Z бесконечно.

а) Пусть E'' — коммутант тела E' в D. Показать, что существует такой элемент $b \in E''$, что $E'' = E(b)$ (подтело, порожденное в D подтелом E и элементом b). (Заметить, что, ввиду упражнения 6, существует лишь конечное число автоморфизмов тела E'', оставляющих инвариантными элементы E; вывести отсюда, что найдется элемент $b \in E''$, неинвариантный при каждом из этих автоморфизмов, и воспользоваться упражнением 6а).)

б) Пусть N — максимальное подполе тела E', сепарабельное над центром $T = E' \cap E''$ тела E'; пусть $N = T(c)$. Показать, что существует лишь конечное число различных элементов $\sigma(c)$, принадлежащих N, когда σ пробегает G. (Свести доказательство к случаю внутренних автоморфизмов $\sigma \in G$ и заметить, что если в этом случае $\sigma(c) \in N$, то $\sigma(N) = N$ и σ оставляет инвариантными элементы T.)

в) Пусть N' — коммутант N в D. Вывести из а) и б), что существует такой элемент $x \in E$, что $N' = E(a)$, где $a = c - xb$ (показать, что при подходящем выборе элемента x не существует внешнего автоморфизма $\sigma \in G$, оставляющего инвариантным a, и применить упражнение 6а)).

г) Показать, что в теле D имеется такой элемент a', что $D = N'(a')$ (использовать упражнение 7б), заменив в нем E на N'); следовательно, $D = E(a, a')$.

9) Пусть K — поле, Z — его циклическое расширение степени $\geqslant 3$ (гл. V, § 11, n°·5), A — алгебра $M_2(Z)$ матриц порядка 2 над Z. Пусть σ — образующий группы Галуа поля Z над K, и C — подкольцо в A, состоящее из матриц $\begin{pmatrix} z & 0 \\ 0 & \sigma(z) \end{pmatrix}$, где $z \in Z$.

а) Показать, что существует такая группа Галуа G автоморфизмов алгебры A, что (в обозначениях из упражнения 6) $I(G) = K$, $(G : G_0) = n$, $S(G) = A$.

б) Показать, что C — простое подкольцо в A, содержащее K, но его коммутант C_0' в A является прямой композицией двух полей, изоморфных Z. Если H — группа автоморфизмов кольца A, оставляющих инвариантными элементы C, то $I(H) = CZ$. Кроме того, существует изоморфизм φ кольца C на Z, который оставляет инвариантными элементы поля K и не может быть продолжен до автоморфизма алгебры A (см. упражнение 6).

10) Пусть K — поле, σ — его автоморфизм, отличный от тождественного, D — множество $K(X)$ формальных степенных рядов от одного переменного X, наделенное такой структурой некоммутативного тела, что $X\lambda = \lambda^{\sigma}X$ для любого $\lambda \in K$ (гл. IV, § 5, упражнение 10); чему равен центр D? Пусть τ — автоморфизм поля K, перестановочный с σ; показать, что существует единственный автоморфизм тела D, продолжающий τ и оставляющий инвариантным X.

Получить отсюда пример автоморфизма некоммутативного тела, оставляющего инвариантными элементы центра, но не внутреннего.

11) Пусть D — тело конечного ранга над своим центром K. Для того чтобы простая алгебра $A = \boldsymbol{M}_n(D)$ содержала подалгебру, изоморфную $\boldsymbol{M}_r(K)$ и имеющую ту же единицу, что и A, необходимо и достаточно, чтобы r делило n (использовать следствие 2 теоремы 2 n° 2).

12) Пусть K — поле, D — тело ранга m^2 над своим центром K. Для того чтобы в алгебре $\boldsymbol{M}_n(K)$ существовало подтело с центром K, изоморфное D, необходимо и достаточно, чтобы m^2 делило n (использовать существование группы Брауэра).

*13) Пусть D, E — тела, центры которых содержат K; предположим, что ранг $[E : K] = m$ конечен и поле K является центром одного из тел D, E. Тогда алгебра $D \otimes E$ изоморфна $\mathscr{L}_C(V)$, где V — векторное пространство конечной размерности h над телом C (§ 7, n° 4, следствие 2 теоремы 2).

а) Показать, что m кратно h (рассмотреть V и $D \otimes E$ как векторные пространства над D и воспользоваться теоремой 2 § 5, n° 4).

б) Для того чтобы тело E было K-изоморфно подалгебре некоторой алгебры вида $\mathscr{L}_D(W)$, где W — векторное пространство над телом D, необходимо и достаточно, чтобы размерность пространства W над D была бесконечной или кратной m/n (заметить, что W есть $(D \otimes E)$-модуль (§ 7, упражнение 1)).

в) Показать, что если ранг $[D : K]$ конечен и независим с $[E : K]$, то $D \otimes E$ — тело (использовать а)).

*14) Пусть D — тело с центром Z, V — векторное пространство над D; отождествим D с телом гомотетий пространства V, содержащимся в кольце Ω эндоморфизмов абелевой группы V. Пусть $A = \mathscr{L}_D(V)$ и B — плотное подкольцо в A, содержащее Z.

Пусть E — подтело в D, содержащее Z, F — его коммутант в D. Показать, что алгебра $B \otimes_Z E$ изоморфна некоторой плотной подалгебре в $\mathscr{L}_F(V)$ (использовать упражнение 19а) § 7 и рассмотреть коммутант в Ω произведения BE). Частный случай — когда E — максимальное подполе тела D (доказать его существование).

*15) Пусть B — простая алгебра конечного ранга над своим центром K, N — расширение Галуа поля K конечной степени n, нейтрализующее для алгебры B; положим $A = B_{(N)} = B \otimes N$ и отождествим A с алгеброй $\mathscr{L}_N(V)$ эндоморфизмов векторного пространства V над N. Пусть C — коммутант алгебры B в кольце Ω эндоморфизмов абелевой группы V, C — простая алгебра с центром K, и N является ее максимальным коммутативным подкольцом. Пусть G — группа Галуа поля N над K и $\sigma \in G$. Положив $(b \otimes x)^\sigma = b \otimes x^\sigma$ для $b \in B$, $x \in N$, автоморфизм σ можно продолжить до автоморфизма алгебры A, оставляющего инвариантными элементы B; эту группу автоморфизмов алгебры A также обозначим через G.

а) В обозначениях упражнения 4 (при $D = Z = N$) выполняются равенства $G_0 = \{1\}$, $U(G) = C$, $I(G) = B$, $S(G) = N$, и G является группой Галуа автоморфизмов алгебры A (упражнение 6). Пусть H_σ^*, где $\sigma \in G$,— множество таких обратимых элементов $u \in C$, что σ есть автоморфизм $z \to uzu^{-1}$ алгебры A; $H_\sigma = H_\sigma^* \cup \{0\}$ — векторное подпространство (левое и правое) в C размерности 1 над полем N, и C является прямой суммой подпространств H_σ. Объединение H^* множеств H_σ^* ($\sigma \in G$) является подгруппой в группе C^* обратимых элементов алгебры C и совпадает с группой элементов $u \in C^*$ таких, что $uNu^{-1} \subset N$; пусть $\varrho(u)$, где $u \in H^*$, есть элемент $\sigma \in G$ такой, что σ есть автоморфизм $z \to uzu^{-1}$ алгебры A; отображение $\varrho \to \varrho(u)$ является гомоморфизмом группы H^* на G, и его ядро есть мультипликативная группа N^*.

б) Обратно, пусть H^* — группа, в которой N^* является истинной подгруппой; предположим, что существует гомоморфизм ϱ группы H^* на группу G с ядром N^*, такой, что $\varrho(u)$ — автоморфизм $x \to uxu^{-1}$ группы N^*. Показать, что тогда существует простая алгебра C с центром K, в которой поле N является максимальным подполем, а H^* — группой обратимых элементов таких, что $uNu^{-1} \subset N$. (Для любого $\sigma \in G$ рассмотреть в H^* обратный образ H_σ^* автоморфизма σ при гомоморфизме ϱ; показать, что на сумме H_σ множеств H_σ^* и $\{0\}$ можно определить структуру векторного пространства размерности 1 над полем N, а затем на векторном пространстве C, прямой сумме H_σ, нужную структуру алгебры относительно K; для доказательства, что C просто, рассуждать, как в упражнении 4г).)

*16) Пусть B, B' — простые алгебры с центром K и конечного ранга над K, обладающие общим нейтрализующим расширением Галуа N поля K; пусть H^*, H'^* — группы, соответствующие этим алгебрам при построении, описанном в упражнении 15, ϱ, ϱ' — соответствующие гомоморфизмы групп H^*, H'^* соответственно на группу Галуа G поля N. Пусть B'' — алгебра $B \otimes B'$, H''^* и ϱ'' — соответствующие ей при том же построении группа и гомоморфизм. Рассмотрим в группе $H^* \times H'^*$ подгруппу J, состоящую из пар (u, u') таких, что $\varrho(u) = \varrho'(u')$, и определим гомоморфизм ϱ_1 группы J на G, положим $\varrho_1(u, u') = \varrho(u) = \varrho'(u')$, $(u, u') \in J$. С другой стороны, пусть S — подгруппа в $N \times N^*$, состоящая из пар (λ, λ^{-1}); показать, что группу H''^* можно канонически отождествить с J/S, а гомоморфизм ϱ'' — с гомоморфизмом группы J/S на G, получаемым из ϱ_1 путем факторизации. (Если $B \otimes N$ и $B' \otimes N$ отождествлены с алгебрами эндоморфизмов $\mathscr{L}_N(V)$ и $\mathscr{L}_N(V')$, то отождествить $B'' \otimes N$ с $\mathscr{L}_N(V \otimes V')$; показать затем, что при всяком $\sigma \in G$ отображение $(u, u') \to u \otimes u'$ группы $H_\sigma^* \times H_\sigma'^*$ в кольцо эндоморфизмов абелевой группы V^* является сюръекцией на $H_\sigma''^*$.)

§ 11. Применения

1. Конечные тела

Теорема 1 (Веддерберн). *Всякое конечное тело — поле.*

Пусть D — конечное тело с центром K, L — его максимальное подполе. Всякое другое максимальное подполе тела D имеет над K ту же степень, что и L (§ 10, n° 3, следствие предложения 3); следовательно, оно K-изоморфно L (гл. V, § 11, n° 4, предложение 3) и имеет вид xLx^{-1}, где $x \in D^*$ (§ 10, n° 1, теорема 1). Так как всякий элемент тела D содержится в некотором максимальном подполе, то мультипликативная группа D^* является объединением подгрупп xL^*x^{-1}, сопряженных L^*; кроме того, если $x' = xt$, $t \in L^*$, то $x'\,L^*\,x'^{-1} = xtL^*\,t^{-1}\,x^{-1} = xL^*x^{-1}$. Поэтому число различных сопряженных подгрупп xL^*x^{-1} *не превышает* числа левых классов xL^* группы D^* по подгруппе L^*. Так как все эти сопряженные подгруппы имеют одно и то же число элементов, то отсюда следует, что D^* может быть объединением подгрупп xL^*x^{-1} только в случае, когда они попарно не пересекаются. Однако их общим элементом является единица группы D^*, и следовательно, должно выполняться равенство $D^* = L^*$, то есть $D = L = K$.

2. Характеризация тел кватернионов

Предложение 1. *Пусть K — поле характеристики $\neq 2$. Всякое некоммутативное надтело D ранга 4 над K, центр которого содержит K, является телом кватернионов над K* (гл. II, § 7, n° 8).

Ранг тела D над своим центром является квадратом (§ 7, n° 4, следствие 3 теоремы 2), следовательно, центр D равен K. Пусть L — максимальное подполе тела D; по следствию предложения 3 § 10, n° 3, $[L : K] = 2$, и, поскольку характеристика поля K не равна 2, L имеет вид $K(u)$, где $u^2 \in K$ (гл. II, § 7, n° 7). По теореме 1 § 10, n° 1, K-автоморфизм ϑ: $\lambda + \mu u \to \lambda - \mu u$ является сужением на $K(u)$ некоторого внутреннего автоморфизма $x \to vxv^{-1}$ тела D. Так как автоморфизм ϑ не тождественный, то $v \notin L$; но ϑ^2 — тождественный автоморфизм, так что v^2 принадлежит коммутанту подполя L в D, то есть L. Более того, $v \in K$: если $v^2 \notin K$, то $L = K(v^2)$ и ϑ — тождественный автоморфизм поля L.

Положим $u^2 = \alpha$, $v^2 = \beta$ и $uv = w$. Тогда $vuv^{-1} = -u$, то есть $uv = -vu$ и $w^2 = uvuv = -u^2v^2 = -\alpha\beta$, $vw = vuv = -uv^2 = -\beta u$, $wv = uv^2 = \beta u$, $wu = uvu = -u^2v = -\alpha v$, $uw = u^2v = \alpha v$. Остается доказать, что элементы 1, u, v, w образуют базис тела D над K. Но в противном случае существуют такие элементы λ, μ, $\nu \in K$, что $w = \lambda + \mu u + \nu v$, следовательно, $(u - \nu)\, v = \lambda + \mu u$, откуда следует, что $v \in K(u) = L$.

Напомним (гл. II, § 7, n° 8), что алгебра кватернионов над полем K характеристики $\neq 2$, соответствующая паре (α, β), не всегда является телом; для этого необходимо и достаточно, чтобы равенство $x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2 = 0$ (где $x_0, x_1, x_2, x_3 \in K$) влекло $x_0 = x_1 = x_2 = x_3 = 0$.

Следствие. *Пусть D — некоммутативное тело конечного ранга над своим центром K. Если для любого $x \in D$ поле $K(x)$ имеет ранг $\leqslant 2$ над K и характеристика поля K отлична от 2, то D — тело кватернионов над K.*

Пусть L — максимальное подполе тела D, сепарабельное расширение поля K (§ 10, n° 3, предложение 4). По предложению 4 гл. V, § 11, n° 4, это расширение моногенно и, по предположению, имеет степень $\leqslant 2$. Следовательно, $[D, K] = 1$ или $[D, K] = 4$ (§ 10, n° 3, следствие предложения 3). Так как D некоммутативно, то $[D : K] = 4$, и можно применить предложение 1.

Пусть K — поле и D — тело кватернионов над K. Изоморфизм $x \to \bar{x}$ тела D на D^0 инволютивен (гл. II, § 7, n° 8), и для любого $x \in D$ элементы $x + \bar{x}$ и $x\bar{x}$ принадлежат центру тела D. Обратно:

Предложение 2. *Пусть D — некоммутативное тело характеристики $\neq 2$, конечного ранга над своим центром K. Пусть $x \to x^J$ — K-изоморфизм тела D на противоположное тело D^0, такой, что при любом $x \in D$ элементы $x + \bar{x}$ и $x\bar{x}$ принадлежат K. Тогда D — тело кватернионов над K, и $x^J = \bar{x}$ для любого $x \in D$.*

В самом деле, для любого $x \in D$ справедливо равенство $x^2 - x(x + x^J) + xx^J = 0$, откуда следует, что поле $K(x)$ имеет над K степень $\geqslant 2$. По следствию предложения 1 D есть тело кватернионов над K. Кроме того, если $x \notin K$, то $X^2 - (x + x^J)\, X + xx^J$ — минимальный многочлен элемента x над полем K в $K(x)$.

Но $x^2 - (x + \bar{x})\,x + x\bar{x}$ также равно 0, откуда следует, что многочлен $X^2 - (x + \bar{x})\,X + x\bar{x}$ является минимальным многочленом элемента x в $K(x)$; поэтому $x^j = \bar{x}$.

Пусть K — упорядоченное поле. Тогда условие $x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0$ влечет $x_0 = x_1 = x_2 = x_3 = 0$, то есть алгебра кватернионов над K, соответствующая паре $(-1, -1)$, является телом. Обратно:

Теорема 2 (Фробениус). *Пусть K — максимальное упорядоченное поле, D — его некоммутативное надтело конечного ранга над K, содержащее K в центре. Тогда D K-изоморфно телу кватернионов над K, соответствующему паре* $(-1, -1)$.

Всякое (коммутативное) алгебраическое расширение поля K имеет степень 1 или 2 (гл. VI, § 2, n° 6, предложение 9); поэтому следствие предложения 1 показывает, что D — тело кватернионов над своим центром C. Так как D — тело, то C не может быть алгебраически замкнутым (§ 4, n° 3, лемма 3). Следовательно, $C = K$. Всякий элемент поля K имеет вид u^2 или $-u^2$, где $u \in K$ (гл. VI, § 2, n° 5, предложение 6); следовательно, алгебра кватернионов a_1 K, соответствующая паре (α, β), может быть телом только в случае, когда $\alpha = -\lambda^2$ и $\beta = -\mu^2$ (гл. II, § 7, n° 8); в этом случае тело D K-изоморфно алгебре кватернионов, соответствующей паре $(-1, -1)$ (гл. II, § 7, n° 8).

Упражнения. 1) Элемент x алгебры A над полем K называется *алгебраическим*, если подалгебра $K[x]$, порожденная этим элементом и 1, имеет конечную размерность; в этом случае идеал алгебраических соотношений, которым удовлетворяет x, имеет вид (f), где f — унитарный многочлен $\neq 0$ из $K[X]$, называемый *минимальным многочленом* элемента x над K; степень f называется *степенью* x над K. Алгебра A называется *алгебраической* над полем K, если всякий ее элемент алгебраичен над K. Всякая алгебра конечного ранга над K алгебраична над K.

а) Показать, что всякая алгебраическая алгебра является псевдорегулярным кольцом (§ 6, упражнение 14) (заметить, что если элемент x алгебраичен над K, то существуют целое число $k \geqslant 0$ и элемент $y \in K[x]$ такой, что $x^k = x^{k+1}y$). Тогда радикал алгебры A будет нильидеалом (§ 6, упражнения 14а) и 13б)). Всякая подалгебра и всякая факторалгебра алгебры A алгебраичны.

б) Пусть D — тело с центром K и все его элементы алгебраичны над K и имеют степень $\leqslant m$. Показать, что $[D : K] \leqslant m^2$ (использовать лемму 1 § 10, n° 3).

в) Пусть A — примитивная алгебраическая алгебра над K (§ 5, упражнение 5) и все ее элементы имеют степень $\leqslant m$ над K. Показать, что A есть алгебра матриц $M_r(D)$ над некоторым телом D, все элементы которого алгебраичны над K и их степени $\leqslant m$; при этом $r \leqslant m$. (Используя теорему плотности (§ 4, n° 2, теорема 1), показать, что если алгебра A не простая, то для любого n в ней найдется подалгебра B_n такая, что некоторая ее факторалгебра изоморфна алгебре матриц $M_n(D_n)$ над некоторым телом D_n, и заметить, что в $M_n(D_n)$ существуют элементы z такие, что $z^{n-1} \neq 0$ и $z^n = 0$.)

г) Пусть A — алгебраическая алгебра без радикала над бесконечным полем K и все ее элементы имеют степень $\leqslant m$ над K. Показать, что A полупроста и имеет не более m простых компонент. (Заметить сначала, что прямая композиция n алгебр над полем K содержит алгебраические элементы степени n над K; затем, применяя индукцию по k и используя в), показать, что если $\mathfrak{a} = \bigcap_i \mathfrak{m}_i$ — пересечение различных максимальных двусторонних идеалов $\mathfrak{m}_i$ $(1 \leqslant i \leqslant k)$ алгебры A, то $A/\mathfrak{a}$ полупроста и имеет k простых компонент. В заключение применить упражнение 7 § 6.) Если поле K совершенно, то алгебра A имеет над K конечный ранг.

2) а) Пусть K — конечное поле. Показать, что если все элементы надтела D алгебраичны над K, то D — поле. (Пусть Z — центр тела D и $Z \neq D$; пусть x — элемент тела D, не принадлежащий Z. Показать, что существует элемент $y \in D$ такой, что $yZ(x)\,y^{-1} = Z(x)$, и сужение на $Z(x)$ отображения $z \to yzy^{-1}$ не является тождественным; рассматривая в D подтело $K(x, y)$ и применяя теорему 1 n° 1, вывести отсюда противоречие.)

б) Показать, что алгебраическая алгебра без ненулевых нильпотентных элементов изоморфна некоторой подалгебре произведения тел. (Рассматривая минимальный многочлен элемента $x \in A$, заметить, что если образ $f(x)$ этого элемента при некотором гомоморфизме f алгебры A в алгебру B нильпотентен и $\neq 0$, то элемент x сам нильпотентен. Затем, рассуждая, как в упражнении 1в), разобрать частный случай, когда алгебра A примитивна. В заключение применить упражнение 1а) и упражнение 7 § 6.)

в) Вывести из а) и б), что алгебраическая алгебра без ненулевых нильпотентных элементов над конечным полем коммутативна.

г) Пусть A — алгебраическая алгебра без радикала над конечным полем K и все ее элементы имеют над K степень $\leqslant m$. Показать, что существует такое расширение E конечной степени поля K, что алгебра A изоморфна подалгебре произведения $(M_r(E))^I$ (I — некоторое множество индексов), все проекции которого — простые алгебры (см. упражнение 1в)). Доказать обратное утверждение.

*3) Пусть A — такое кольцо, что для всякого $x \in A$ существует целое число $n(x) > 1$, удовлетворяющее условию $x^{n(x)} = x$. Показать, что A является прямой композицией конечного числа алгебраических алгебр без нильпотентных элементов $\neq 0$ над конечными полями и, следовательно, коммутативных (упражнение 2в)). (Заметить сначала, что для любых двух элементов x, $y \in A$ существует целое число $r > 1$ такое, что $x^r = x$ и $y^r = y$. Вывести отсюда, что аддитивная группа A является группой кручения, а ее p-компоненты A_p (гл. VII, § 2, n° 2) — двусторонними идеалами кольца A; показать, кроме того, что для любого $x \in A_p$ выполняется равенство $px = 0$.)

4) Пусть D — некоммутативное тело с центром K и для всякого $x \in D$ подполе $K(x)$ имеет над K ранг $\leqslant 2$.

а) Показать, что если характеристика тела D не равна 2, то D — тело кватернионов над K (см. упражнение 1б)).

б) Показать, что если характеристика тела D равна 2, то в нем имеется базис $(1, u, v, w)$ над полем K такой, что

$$u^2 = \alpha, \quad v^2 = v + \beta, \quad uv = w, \quad vu = w + u,$$
$$w^2 = \alpha\beta, \quad vw = \beta u, \quad wv = \beta u + w, \quad wu = \alpha + \alpha v, \quad uw = \alpha v,$$

где $\alpha \in K$, $\beta \in K$. Обратно, указанная выше таблица умножения при любых α, $\beta \in K$ определяет алгебру A с центром K и ранга 4 над K. K-линейное отображение $x \to \bar{x}$ алгебры A на себя, определенное равенствами $\bar{1} = 1$, $\bar{u} = u$, $\bar{v} = v + 1$, $\bar{w} = w$, является изоморфизмом A на противоположную алгебру A^0, при котором элементы $x + \bar{x}$ и $\bar{x}x = x\bar{x}$ принадлежат K. Для того чтобы алгебра A была телом, необходимо и достаточно, чтобы равенство

$$x_1^2 + x_0x_2 + \beta x_2^2 + \alpha(x_1^2 + x_1x_3 + \beta x_3^2) = 0,$$

где $x_i \in K$ $(0 \leqslant i \leqslant 3)$, влекло $x_0 = x_1 = x_2 = x = 0$; в частности, α и $\alpha\beta$ не должны быть квадратами в поле K (что невозможно, если поле K несовершенно) и многочлен $X^2 + X + \beta$ должен быть неприводим над K (см. § 12, упражнение 6).

в) Пусть K_0 — поле характеристики 2, $K = K_0(X, Y)$ — поле рациональных дробей от двух переменных над полем K. Показать, что алгебра A над полем K, имеющая таблицу умножения, описанную в б), при $\alpha = X$, $\beta = Y$ является телом.

г) Пусть D — некоммутативное тело с центром K, $x \to x^J$ — K-изоморфизм тела D на D^0, при котором элементы $x + x^J$ и xx^J для всех $x \in D$ лежат в K. Показать, что если характеристика поля K не равна 2, то D — тело кватернионов над K, если же характеристика поля K равна 2, то D — тело типа, описанного в б); показать также, что $x^J = \bar{x}$ для любого $x \in D$; такое тело называется *рефлексивным*.

*5) а) Пусть D — тело с центром Z, и $A = M_r(D)$ — простая алгебра конечного ранга над полем K; пусть $x \to x^J$ — K-изомор-

физм A на противоположную алгебру A^0 такой, что $(x^J)^J = x$ для любого $x \in A$ (*инволютивный антиавтоморфизм* алгебры A). Элемент $a \in A$ называется *J-симметрическим* (соответственно *J-антисимметрическим*), если $a^J = a$ (соответственно $a^J = -a$). Пусть $x \to x^T$ — другой инволютивный антиавтоморфизм алгебры A такой, что $x^T = x^J$ для всех $x \in Z$. Показать, что существует обратимый элемент $a \in A$, J-симметрический или J-антисимметрический, такой, что $x^T = ax^J a^{-1}$ для любого $x \in A$ (см. § 10, n° 1, теорема 1 и гл. V_t § 11, n° 5, теорема 3). Доказать обратное утверждение.

б) Показать, что существуют такой инволютивный антиавтоморфизм $x \to x^T$ алгебры A и такой K-изоморфизм алгебры A на тензорное произведение $D \otimes_Z \boldsymbol{M}_r(Z)$, что $x^T = x^J$ для всех $x \in Z_r$ и после отождествления алгебры A с тензорным произведением посредством этого изоморфизма сужение отображения $x \to x^T$ на D — антиавтоморфизм D, а сужение отображения $x \to x^T$ на $\boldsymbol{M}_r(Z)$ есть $X \to {}^t X^J$ (рассмотреть образы канонического базиса алгебры $\boldsymbol{M}_r(Z)$ при отображении $x \to x^J$ и рассуждать, как в а)).

в) Антиавтоморфизм J называется антиавтоморфизмом *первого рода*, если он оставляет инвариантным каждый элемент поля Z, и *второго рода* — в противоположном случае. Пусть $[A : Z] = m^2$. Показать, что если антиавтоморфизм J второго рода, то множество S (соответственно T) J-симметрических (соответственно J-антисимметрических элементов алгебры A является векторным пространством размерности m^2 над подполем Z_0 поля Z, причем Z — сепарабельное квадратичное расширение этого подполя; показать также, что базис S над Z_0 будет базисом A над Z (рассмотреть Z_0-линейное отображение $x \to x - x^J$ алгебры A в себя). Кроме того, если характеристика поля K не равна 2, то Z_0-пространство A является прямой суммой S и N.

г) Показать, что если антиавтоморфизм J первого рода, то S есть векторное пространство размерности $m(m+1)/2$ или $m(m-1)/2$ над Z (распространить J на алгебру $A_{(L)}$, где L — нейтрализующее поле алгебры A, и применить а) и б)). Кроме того, если характеристика поля K не равна 2, то A является прямой суммой S и N.

6) Пусть A — алгебра кватернионов над полем K характеристики $\neq 2$, соответствующая паре (α, β); для любого элемента $x \in A$ положим $N(x) = x\bar{x} = \bar{x}x$; известно, что $N(x) \in K$.

а) *Чистым кватернионом* называется всякий элемент алгебры A, антисимметрический относительно антиавтоморфизма $x \to \bar{x}$ (упражнение 5а)); показать, что если кватернион z чистый, то кватернион tzt^{-1} чистый при любом обратимом $t \in A$.

б) Показать, что если существует такой кватернион $z \neq 0$, что $N(z) = 0$, то существует и чистый кватернион $z' \neq 0$ такой, что $N(z') = 0$. (Заметить (обозначения из n° 2), что если элемент a не

является в поле K квадратом, то существование кватерниона $z \neq 0$, для которого $N(z) = 0$, равносильно существованию такого элемента $y \in K(u)$, что $\beta = N(y)$.)

7) а) Пусть D — тело, N — его подтело. Показать, что если мультипликативная группа N^* имеет в D^* конечный индекс, то либо D конечно (и, следовательно, коммутативно), либо $N = D$. (В случае, когда N бесконечно, рассмотреть бесконечную последовательность (a_n) различных его элементов и для любого $x \in D - N$ классы элементов $x + a_n$ по mod N^*.)

б) Показать, что всякий элемент x группы D^*, имеющий лишь конечное число сопряженных в этой группе, принадлежит центру Z тела D (рассмотреть подтело, коммутант элемента x в D, и применить а)).

в) Вывести из б), что если некоторый многочлен $f \in Z[X]$ имеет хотя бы один корень в $D - Z$, то он имеет в этом множестве бесконечно много корней.

§ 12. Нормы и следы

1. *Норма и след относительно модуля*

Определение 1. *Пусть K — коммутативное кольцо, A — алгебра над K, M — A-модуль; предположим, что M является свободным K-модулем конечной размерности* *) *относительно структуры, определяем на нем сужением на K кольца скаляров. Характеристическим многочленом* (соответственно *нормой, следом*) *произвольного элемента $a \in A$ относительно A-модуля M называется характеристический многочлен* **) (соответственно *определитель, след* (гл. III, § 4, n° 5)) *эндоморфизма $a_M : x \to ax$ K-модуля M; этот элемент кольца $K[X]$* (соответственно *кольца K*)

---

*) Напомним, что если модуль M над коммутативным кольцом K имеет конечный базис, то все его базисы над K имеют одно и то же число элементов, называемое *размерностью* M над K (гл. III, приложение II, n° 11). С другой стороны, рассуждение, такое же, как в теореме 2 § 3, n° 5, показывает, что если модуль M имеет над K бесконечный базис B, то всякий его другой базис B' равномощен B; Card (B) также называют *размерностью* M над K.

**) Определение характеристического многочлена матрицы над некоторым телом, данное в гл. VII, § 5, n° 3, определение 4, легко распространяется на квадратные матрицы над произвольным коммутативным кольцом K и, следовательно, на произвольный эндоморфизм свободного K-модуля конечной размерности.

обозначается $\mathrm{Pc}_{M/K}(a;\ X)$ (соответственно $\mathrm{N}_{M/K}(a)$, $\mathrm{Tr}_{M/K}(a)$) *или просто* $\mathrm{Pc}_M(a;\ X)$ (соответственно $\mathrm{N}_M(a)$, $\mathrm{Tr}_M(a)$).

Из этого определения немедленно следует, что для любых элементов $a,\ a' \in A$ выполняются равенства

$$\mathrm{Tr}_M(a+a') = \mathrm{Tr}_M(a) + \mathrm{Tr}_M(a'), \quad \mathrm{N}_M(aa') = \mathrm{N}_M(a)\,\mathrm{N}_M(a'), \tag{1}$$

$$\mathrm{Tr}_M(a'a) = \mathrm{Tr}_M(aa') \tag{2}$$

(см. гл. III, § 4, n° 5, предложение 2).

Пусть $(m_{ij}(a))$ — матрица эндоморфизма $x \to ax$ относительно некоторого базиса K-модуля M, тогда

$$\mathrm{Tr}_M(a) = \sum_i m_{ii}(a), \quad \mathrm{N}_M(a) = \det(m_{ij}(a)),$$
$$\mathrm{Pc}_M(a;\ X) = \det(\delta_{ij}X - m_{ij}(a)), \tag{3}$$

откуда, положив $n = \dim_K M$ и $\mathrm{Pc}_M(a;\ X) = X^n + c_{n-1}X^{n-1} + \ldots + c_0$, получим

$$c_{n-1} = -\mathrm{Tr}_M(a), \quad c_0 = (-1)^n \mathrm{N}_M(a). \tag{4}$$

Для любого $\lambda \in K$ имеем равенства

$$\mathrm{Tr}_M(\lambda) = n\lambda, \quad \mathrm{N}_M(\lambda) = \lambda^n, \quad \mathrm{Pc}_M(\lambda;\ X) = (X-\lambda)^n. \tag{5}$$

Предложение 1. *Пусть* $M = M_0 \supset M_1 \supset \ldots \supset M_r = \{0\}$ — *композиционный ряд* A-*модуля* M; *предположим, что каждый из фактормодулей* $V_i = M_{i-1}/M_i$ *является свободным* K-*модулем конечной размерности* $(1 \leqslant i \leqslant r)$. *Для любого элемента* $a \in A$ *справедливы равенства*

$$\mathrm{Tr}_M(a) = \sum_i \mathrm{Tr}_{V_i}(a), \quad \mathrm{N}_M(a) = \prod_i \mathrm{N}_{V_i}(a),$$
$$\mathrm{Pc}_M(a;\ X) = \prod_i \mathrm{Pc}_{V_i}(a;\ X).$$

Пусть B_i' — базис модуля V_i над K; тогда система представителей B_i классов B_i' $(\mathrm{mod}\ M_i)$ является базисом дополнения K-модуля M_i в K-модуле M_{i-1} (гл. II, § 1, n° 6, предложение 4). В качестве базиса модуля M над K возьмем объединение $B = B_r \cup B_{r-1} \cup \ldots \cup B_1$ базисов B_i. Пусть X_{ii} — матрица эндоморфизма a_{V_i} относительно базиса B_i'. Так как модуль M_{i-1} является подмодулем в A-модуле M и имеет базис $B_r \cup B_{r-1} \cup \ldots \cup B_i$, то матрица эндоморфизма a_M относительно базиса B

имеет вид

$$\begin{pmatrix} X_{rr} & X_{r,r-1} & \dots & X_{r1} \\ 0 & X_{r-1,r-1} & \dots & X_{r-1,1} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & X_{11} \end{pmatrix}$$

и предложение вытекает из формул (3) и формулы (16) гл. III, § 6, n° 4.

Предложение 2. *Пусть A, A' — алгебры над коммутативным кольцом K, M — A-модуль, M' — A'-модуль, M и M' свободны над K и имеют размерности n и n'. Если рассматривать $M \otimes M'$ как $(A \otimes A')$-модуль* *), то для $a \in A$, $a' \in A'$*

$$\begin{aligned} \mathrm{Tr}_{M\otimes M'}(a \otimes a') &= \mathrm{Tr}_M(a)\,\mathrm{Tr}_{M'}(a'), \\ N_{M\otimes M'}(a \otimes a') &= (N_M(a))^{n'}\,(N_{M'}(a'))^{n}. \end{aligned} \tag{6}$$

Надо доказать следующую лемму:

Лемма 1. *Пусть V, V' — свободные K-модули размерности n, n', u — эндоморфизм модуля V, u' — эндоморфизм модуля V'. Тогда*

$$\mathrm{Tr}(u \otimes u') = \mathrm{Tr}(u)\,\mathrm{Tr}(u'), \qquad \det(u \otimes u') = (\det(u))^{n'}\,(\det(u'))^{n}. \tag{7}$$

В самом деле, пусть X, X' — матрицы эндоморфизмов u и u' относительно некоторых базисов (e_i) и (e'_i) модулей V и V' соответственно; тогда матрица эндоморфизма $u \otimes u'$ относительно базиса $(e_i \otimes e'_j)$ модуля $V \otimes V'$ будет тензорным произведением $X \otimes X'$ (гл. III, § 1, n° 6); отсюда немедленно следует первая из формул (7). Для доказательства второй формулы заметим, что можно записать равенство $u \otimes u' = (u \otimes 1)\,(1 \otimes u')$ и, таким образом, свести доказательство к случаю, когда один из эндоморфизмов u, u' тождественный. Но если, например, $u' = 1$, то матрица $X \otimes X'$ имеет вид

$$\begin{pmatrix} X & 0 & \dots & 0 \\ 0 & X & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & X \end{pmatrix}$$

*) Определение, данное в § 7, n° 1, для алгебр A и B над телом K, легко распространяется на алгебры A и B над произвольным коммутативным кольцом.

(состоящая из матриц таблица с n' строками и n' столбцами), и по формуле (16) гл. III, § 6, n° 4, $\det(X \otimes X') = (\det(X))^n$.

Замечание. Для выражения характеристического многочлена элемента $a \otimes a'$ относительно $M \otimes M'$ простой формулы нет (см. гл. VII, § 5, n° 6, предложение 14). Но при $a' = 1$ имеем равенство

$$\mathrm{Pc}_{M\otimes M'}(a \otimes 1;\ X) = (\mathrm{Pc}_M(a;\ X))^{n'};$$

это равенство вытекает из предыдущего рассуждения.

Пусть L — коммутативное кольцо, содержащее K и имеющее ту же единицу, что и K. Модуль $M_{(L)} = M \otimes L$ над алгеброй $A_{(L)} = A \otimes L$ является свободным L-модулем; более точно, если (e_i) — базис модуля M над K, то $(e_i \otimes 1)$ — базис $M_{(L)}$ над K (гл. III, § 2, n° 2, теорема 1). Тогда для любого a

$$\begin{gathered}\mathrm{Tr}_{M_{(L)}}(a \otimes 1) = \mathrm{Tr}_M(a), \qquad \mathrm{N}_{M_{(L)}}(a \otimes 1) = \mathrm{N}_M(a), \\ \mathrm{Pc}_{M_{(L)}}(a \otimes 1;\ X) = \mathrm{Pc}_M(a;\ X).\end{gathered} \tag{8}$$

Из формул (3) при $L = K[X]$ сразу же следует равенство

$$\mathrm{Pc}_M(a;\ X) = \mathrm{N}_{M_{(K[X])}}(X - a), \tag{9}$$

откуда, заменяя X на $-1/X$, получаем

$$\mathrm{N}_{M(K[X])}(1 + aX) = 1 + (\mathrm{Tr}_M(a))\,X + \ldots + (N_M(a))\,X^n. \tag{10}$$

Если K — поле, то в предыдущих формулах можно заменить $K[X]$ на поле рациональных дробей $K(X)$.

Пусть A-модули M и M' *изоморфны*. Тогда для любого $a \in A$ выполняются равенства

$$\mathrm{Tr}_{M'}(a) = \mathrm{Tr}_M(a), \qquad \mathrm{N}_{M'}(a) = \mathrm{N}_M(a), \qquad \mathrm{Pc}_{M'}(a;\ X) = \mathrm{Pc}_M(a;\ X);$$

это следует из того, что если f — A-изоморфизм модуля M на M', то матрица эндоморфизма a_M относительно базиса B модуля M над K совпадает с матрицей эндоморфизма $a_{M'}$ относительно базиса $f(B)$. Обратное утверждение имеет место в частном случае:

Предложение 3. *Пусть K — поле характеристики 0, и M, M' — полупростые A-модули конечной размерности над K. Если $\mathrm{Tr}_M(a) = \mathrm{Tr}_{M'}(a)$ для любого $a \in A$, то M и M' — изоморфные A-модули.*

Пусть $\mathfrak{S}$ — множество классов простых A-модулей (§ 3, n° 2), и для любого $\lambda \in \mathfrak{S}$ пусть N_λ (соответственно N'_λ) — изотипная компонента типа λ модуля M (соответственно M'); так как M и M' имеют конечную размерность над K, то N_λ (соответственно N'_λ) будет прямой суммой конечного числа n_λ (соответственно n'_λ) A-модулей, изоморфных λ, и $n_\lambda = n'_\lambda = 0$ для всех λ, кроме элементов некоторого конечного подмножества $H \subset \mathfrak{S}$. Так как A-модули $\lambda \in H$ являются конечномерными векторными K-пространствами, то их контрмодули — конечного типа. Следовательно, для любых $\lambda \in H$, $a \in A$ существует элемент $c \in A$ такой, что $c_\lambda = a_\lambda$ и $c_\mu = 0$ для всех $\mu \neq \lambda$ таких, что $\mu \in H$ (§ 4, n° 2, следствие 2 теоремы 1). Тогда по предложению 1 соотношение $\mathrm{Tr}_M(c) = \mathrm{Tr}_{M'}(c)$ записывается в виде $(n_\lambda - n'_\lambda)\,\mathrm{Tr}_\lambda(a) = 0$. В частности, при $a = 1$ это равенство дает $(n_\lambda - n'_\lambda)\dim_K(\lambda) = 0$, и поскольку характеристика поля K равна 0, то $n_\lambda = n'_\lambda$ для всех $\lambda \in H$, что и заканчивает доказательство.

2. *Норма и след в алгебре*

Определение 2. *Пусть K — коммутативное кольцо, A — алгебра над K, являющаяся свободным M-модулем конечной размерности. Характеристическим многочленом* (соответственно *нормой, следом*) *произвольного элемента $a \in A$ относительно A и K называется характеристический многочлен* (соответственно *норма, след*) *элемента a относительно A-модуля A_s.*

Если не может возникнуть недоразумения, то в этих обозначениях вместо A_s пишут A, а A и K опускают.

Замечание. Если A — алгебра матриц $M_r(K)$, то след $\mathrm{Tr}_{A/K}(x)$ некоторой матрицы $x \in A$ *не равен*, вообще говоря, следу $\mathrm{Tr}(x)$, определенному в гл. III, § 4, n° 5 (см. ниже n° 3).

Пусть $A = A_1 \times A_2 \times \ldots \times A_n$ — произведение n алгебр конечной размерности над K. По предложению 1 n° 1 для любого элемента $a = (a_1, \ldots, a_n)$ алгебры A имеем равенства:

$$\mathrm{Tr}_{A/K}(a) = \sum_{i=1}^{n} \mathrm{Tr}_{A_i/K}(a_i), \qquad \mathrm{N}_{A/K}(a) = \coprod_{i=1}^{n} \mathrm{N}_{A_i/K}(a_i),$$
$$\mathrm{Pc}_{A/K}(a;\ X) = \coprod_{i=1}^{n} \mathrm{Pc}_{A_i/K}(a_i;\ X). \tag{11}$$

Пусть A, A' — алгебры конечной размерности n, n' над K; предложение 2 n° 1 показывает, что при $a \in A$, $a' \in A'$

$$\begin{aligned} \mathrm{Tr}_{A\otimes A'}(a\otimes a') &= \mathrm{Tr}_A(a)\,\mathrm{Tr}_{A'}(a'), \\ \mathrm{N}_{A\otimes A'}(a\otimes a') &= (\mathrm{N}_A(a))^{n'}(\mathrm{N}_{A'}(a'))^n. \end{aligned} \tag{12}$$

Наконец, пусть A — алгебра конечной размерности над K, и L — коммутативное кольцо, содержащее K и имеющее ту же единицу, что и K; отождествим канонически алгебру A с подкольцом в $A_{(L)}$; тогда по формулам (8) для любого $a \in A$

$$\begin{gathered} \mathrm{Tr}_{A_{(L)}/L}(a) = \mathrm{Tr}_{A/K}(a), \qquad \mathrm{N}_{A_{(L)}/L}(a) = \mathrm{N}_{A/K}(a), \\ \mathrm{Pc}_{A_{(L)}/L}(a;\ X) = \mathrm{Pc}_{A/K}(a;\ X). \end{gathered} \tag{13}$$

Предложение 4. *Пусть K — поле, p — его характеристическая экспонента, L — алгебраическое расширение конечной степени поля K, s_i $(1 \leqslant i \leqslant q)$ — различные K-изоморфизмы L в алгебраическое замыкание Ω поля K, и p^e — несепарабельный множитель степени поля L над K* (гл. V, § 8, n° 4). *Для любого $x \in L$ выполняются равенства*

$$\mathrm{Pc}_{L/K}(x;\ X) = \Big(\prod_{i=1}^{q}(X - s_i(x))\Big)^{p^e}, \tag{14}$$

$$\mathrm{Tr}_{L/K}(x) = p^e \sum_{i=1}^{q} s_i(x), \quad \mathrm{N}_{L/K}(x) = \Big(\prod_{i=1}^{q} s_i(x)\Big)^{p^e}. \tag{15}$$

Формулы (15) немедленно следуют из (14) и (4), и достаточно доказать формулы (14). Пусть $r(X)$ — минимальный многочлен элемента x над K; так как r неприводим и $\mathrm{Pc}_{L/K}(x;\ X)$ делит степень $r(X)$ (гл. VII, § 5, n° 3, следствие 1 предложения 8; заметим, что L отождествляется с полем гомотетий векторного пространства L над K), то $\mathrm{Pc}_{L/K}(x;\ X) = (r(X))^f$; так как $\mathrm{Pc}_{L/K}(x;\ X)$ имеет степень $[L : K]$, то

$$f \cdot [K(x) : K] = [L : K]. \tag{16}$$

Пусть m — наименьшее целое число $\geqslant 0$ такое, что элемент x^{p^m} сепарабелен над K; тогда, поскольку $E = K(x^{p^m})$ сепарабельно над K, поле E является наибольшим сепарабельным расширением поля K, содержащимся в $K(x)$; $K(x)$ — радикальное расширение поля E в силу равенства $K(x) = E(x)$ и радикальности элемента x

над E; наше утверждение следует тогда из предложения 5 гл. V, § 8, n° 3. Пусть σ_j $(1 \leqslant j \leqslant s)$ — различные K-изоморфизмы поля E на подполя в Ω; будем предполагать, что каждый σ_j продолжен до K-автоморфизма $\bar{\sigma}_j$ поля Ω; элементы $\sigma_j(x^{p^m})$ — различные сопряженные элементы к x^{p^m} над K; справедливо равенство

$$r(X) = \Big(\prod_{j=1}^{s} (X - \bar{\sigma}_j(x))\Big)^{p^m}. \tag{17}$$

В самом деле, пусть $r_1(X)$ — многочлен из правой части формулы (17); $r_1(X) = \prod_{j=1}^{s} (X^{p^m} - \sigma_j(x^{p^m}))$, следовательно, $r_1 \in K[X]$ и $r_1(x) = 0$; с другой стороны,

$$[K(x) : K] = [K(x) : E]\,[E : K] = p^m s; \tag{18}$$

следовательно, r и r_1 имеют одинаковую степень, откуда и следует (17). Поэтому

$$\mathrm{Pc}_{L/K}(x;\ X) = \Big(\prod_{j=1}^{s} (X - \bar{\sigma}_j(x))\Big)^{tp^m}. \tag{19}$$

Пусть L_0 — наибольшее сепарабельное расширение поля K, содержащееся в L; тогда $E \subset L_0$ и

$$[L : K] = stp^e, \tag{20}$$

где $t = [L_0 : E]$; таким образом, из равенств (16), (18), (19) и (20) следует равенство

$$\mathrm{Pc}_{L/K}(x;\ X) = \Big(\prod_{j=1}^{s} (X - \bar{\sigma}_j(x))\Big)^{tp^e}. \tag{21}$$

Пусть τ_k $(1 \leqslant k \leqslant t)$ — различные E-изоморфизмы поля L_0 на подполя в Ω; каждый из них единственным образом продолжается до E-изоморфизма поля L (он также обозначается через τ_k) на подполе Ω; совершенно очевидно, что K-изоморфизмы $\bar{\sigma}_j \circ \tau_k$ $(1 \leqslant j \leqslant s,\ 1 \leqslant k \leqslant t)$ являются $q = st$ различными K-изоморфизмами поля L на подполя в Ω. Однако x радикален над E, так что $\tau_k(x) = x$ при $1 \leqslant k \leqslant t$; следовательно, $\bar{\sigma}_j(\tau_k(x)) = \bar{\sigma}_j(x)$ при $1 \leqslant k \leqslant t$, и формула (14) является лишь иной записью формулы (21).

Из предложения 4 следует, что в случае, когда L является *сепарабельным* алгебраическим расширением поля K, понятия нормы и следа, определенные в этом параграфе, *совпадают* с теми, которые определены в гл. V, § 10, n° 6. Заметим также, что если поле L не сепарабельно над K, то $\mathrm{Tr}_{L/K}(x) = 0$ для всех $x \in L$.

Предложение 5. *Пусть K — поле, A — алгебра конечной размерности n над K, $x \in A$, $F(x) = \mathrm{Pc}_{A/K}(x; X)$ — характеристический многочлен элемента x. Тогда*

$$\det(\mathrm{Tr}_{A/K}(x^{i+j})) = (-1)^{n(n-1)/2}\,\mathrm{N}_{A/K}(F'(x)) \quad (1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n). \tag{22}$$

Разложим многочлен $F(X) = \prod_{k=1}^{n}(X - a_k)$ в алгебраическом замыкании Ω поля K и рассмотрим определитель Вандермонда $\Delta = \det(a_k^i)$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$; умножив матрицу (a_k^i) на ее транспонированную, получим матрицу, у которой элемент с индексами (i, j) равен $\sum_{k=1}^{n} a^{i+j}$; но по формуле (4) n° 1 и предложению 13 гл. VII, § 5, n° 5, этот элемент представляет собой не что иное, как $\mathrm{Tr}_{A/K}(x^{i+j})$. Следовательно, $\Delta^2 = \det(\mathrm{Tr}_{A/K}(x^{i+j}))$. С другой стороны, по второй формуле (4) n° 1 и по предложению 13 гл. VII, § 5, n° 5, имеем равенство $\mathrm{N}_{A/K}(F'(x)) = \prod_{k=1}^{n} F'(a_k)$; так как $F'(a_k) = \prod_{h \neq k}(a_k - a_h)$, то

$$\prod_{k=1}^{n} F'(a_k) = (-1)^{n(n-1)/2}\Big(\prod_{h<k}(a_k - a_h)\Big)^2,$$

и таким образом, формула (22) следует из выражения для определителя Вандермонда (гл. III, § 6, n° 4, формула (13)).

Предложение 6. *Пусть A — алгебра конечной размерности над полем K, и $\mathfrak{m}$ — такой ее нильпотентный двусторонний идеал, что $D = A/\mathfrak{m}$ — тело. Тогда $[A : K] = r\,[D : K]$, где r — целое число; обозначая через $x \to \tilde{x}$ канонический гомоморфизм алгебры A на $A/\mathfrak{m} = D$, для любого $x \in A$ будем иметь равенства:*

$$\mathrm{Tr}_{A/K}(x) = r\,\mathrm{Tr}_{D/K}(\tilde{x}), \qquad \mathrm{N}_{A/K}(x) = (\mathrm{N}_{D/K}(\tilde{x}))^r,$$
$$\mathrm{Pc}_{A/K}(x; X) = (\mathrm{Pc}_{D/K}(\tilde{x}; X))^r. \tag{23}$$

Пусть n — наименьшее целое число такое, что $\mathfrak{m}^n = \{0\}$; тогда $A_s \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \ldots \supset \mathfrak{m}^{n-1} \supset \mathfrak{m}^n = \{0\}$ есть композиционный ряд A-модуля A_s; далее, так как идеал $\mathfrak{m}$ содержится в аннуляторе A-модуля $V_i = \mathfrak{m}^{i-1}/\mathfrak{m}^i$, то V_i можно рассматривать как левое векторное пространство над телом $D = A/\mathfrak{m}$. Отсюда следует, прежде всего, что $[V_i : K] = r_i\,[D : K]$, где r — целое число, и, следовательно, $[A : K] = \sum_{i=1}^{n} [V_i : K] = r\,[D : K]$, где $r = \sum_{i=1}^{n} r_i$. Кроме того, A-модуль V_i можно отождествить с тензорным произведением $D \otimes_K W_i$, где W_i — векторное пространство размерности r_i над полем K, причем структура A-модуля на этом тензорном произведении определяется структурой A-модуля D. Но при каноническом отождествлении алгебры A с $A \otimes K$ структура A-модуля $D \otimes W_i$ отождествляется с его структурой $(A \otimes K)$-модуля. Тогда из формул (6) n° 1 следуют равенства:

$$\mathrm{Tr}_{V_i}(x) = \mathrm{Tr}_{D\otimes W_i}(x \otimes 1) = r_i\,\mathrm{Tr}_D(x),$$

$$\mathrm{N}_{V_i}(x) = \mathrm{N}_{D\otimes W_i}(x \otimes 1) = (\mathrm{N}_D(x))^{r_i},$$

выполняющиеся для любого $x \in A$; при этом, если x, y — элементы алгебры A, то, по определению, $\widetilde{xy} = \widetilde{\widetilde{x}\widetilde{y}}$ в D, и следовательно, $\mathrm{Tr}_D(x) = \mathrm{Tr}_D(\widetilde{x})$ и $\mathrm{N}_D(x) = \mathrm{N}_D(\widetilde{x})$, что и заканчивает доказательство первых двух формул (23). Третья формула выводится аналогично из замечания к предложению 2 n° 1.

Предложение 7. *Пусть K — коммутативное кольцо, A — коммутативная алгебра над K, имеющая над K конечный базис $(a_i)_{1\leqslant i\leqslant m}$, V — A-модуль, имеющий над A конечный базис $(e_j)_{1\leqslant j\leqslant n}$. Тогда $(a_i e_j)$ является базисом V, рассматриваемого как K-модуль. Если u — A-эндоморфизм модуля V, и u_K — отображение u, рассматриваемое как K-эндоморфизм V, то*

$$\begin{aligned} \mathrm{Tr}(u_K) &= \mathrm{Tr}_{A/K}(\mathrm{Tr}(u)), \qquad \det(u_K) = \mathrm{N}_{A/K}(\det(u)), \\ \mathrm{Pc}(u_K;\ X) &= \mathrm{N}_{A[X]/K[X]}(\mathrm{Pc}(u;\ X)). \end{aligned} \tag{24}$$

Первое утверждение проверяется непосредственно (рассуждением таким же, как в предложении 1 гл. II, § 5, n° 1; заметим,

что в этом рассуждении не используется ни коммутативность алгебры A, ни конечность базисов). Третья формула (24) получается из второй, если применить ее к эндоморфизму $X \otimes \bar{u}$ $A[X]$-модуля $A[X] \otimes_A V$ (гл. VII, приложение, n° 1). Таким образом, достаточно доказать две первые формулы (24).

Мы докажем сначала следующую лемму:

Лемма 2. *Пусть* X_{ij} $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$ — n^2 *переменных,* X — *квадратная матрица* (X_{ij}) *порядка* n, $D(X_{11}, \ldots, X_{nn}) \in \mathbf{Z}[X_{11}, \ldots, X_{nn}]$ — *определитель матрицы* X. *С другой стороны, пусть* A — *коммутативное кольцо,* M_{ij} $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$ — n^2 *квадратных матриц порядка* m *над* A, попарно перестановочных между собой, *и* M — *квадратная матрица порядка* mn *над кольцом* A, *имеющая вид квадратной таблицы из матриц*

$$M = \begin{pmatrix} M_{11} & M_{12} \ldots M_{1n} \\ M_{21} & M_{22} \ldots M_{2n} \\ \ldots\ldots\ldots \\ M_{n1} & M_{n2} \ldots M_{nn} \end{pmatrix}$$

гл. II, § 6, n° 4). *Тогда определитель матрицы* M *равен определителю квадратной матрицы* $D(M_{11}, \ldots, M_{nn})$ *порядка* m.

Проведем индукцию по n; случаи $n = 0$ и $n = 1$ тривиальны. Пусть Z — новая переменная и N_{ij} — матрица $M_{ij} + \delta_{ij} Z I_m$. Если $D^{ij}(X_{11}, \ldots, X_{nn})$ — алгебраическое дополнение элемента X_{ij} в матрице X, то

$$\sum_{i=1}^{n} X_{ji} D^{ik}(X_{11}, \ldots, X_{nn}) = \delta_{jk} D(X_{11}, \ldots, X_{nn}) \tag{25}$$

(гл. III, § 6, n° 4). Положим $N'_{ij} = D^{ij}(N_{11}, \ldots, N_{nn})$; N'_{ij} — матрица порядка m над $A[Z]$. Рассмотрим произведение UN, где

$$U = \begin{pmatrix} N'_{11} & N'_{12} \ldots N'_{1n} \\ 0 & I_m \ldots 0 \\ \ldots\ldots\ldots \\ 0 & 0 \quad\ I_m \end{pmatrix}, \qquad N = \begin{pmatrix} N_{11} & N_{12} \ldots N_{1n} \\ N_{21} & N_{22} \ldots N_{2n} \\ \ldots\ldots\ldots \\ N_{n1} & N_{n2} \ldots N_{nn} \end{pmatrix}.$$

Вычисляя это произведение поклеточно (гл. II, § 6, n° 4) и

пользуясь формулами (25), получим

$$UN = \begin{pmatrix} P & 0 & \dots & 0 \\ N_{21} & N_{22} & \dots & N_{2n} \\ \dots & \dots & \dots & \dots \\ N_{n1} & N_{n2} & \dots & N_{nn} \end{pmatrix},$$

где положено $P = D(N_{11}, \dots, N_{nn})$. Пусть

$$Q = \begin{pmatrix} N_{22} & \dots & N_{2n} \\ \dots & \dots & \dots \\ N_{n2} & \dots & N_{nn} \end{pmatrix}.$$

— матрица порядка m $(n-1)$; имеем равенства $(\det U)(\det N) = (\det P)(\det Q)$ и $\det U = \det N'_{11}$ (гл. III, § 6, n° 4, формула (14)). Но, по предположению индукции, $\det Q = \det(D^{11}(N_{11}, \dots, N_{nn})) = \det N'_{11}$, откуда, по определению N_{ij}, ясно, что Q — *унитарный* многочлен из кольца $A[Z]$ степени $m(n-1)$ и, следовательно, не является в $A[Z]$ делителем 0. Отсюда $\det N = \det(D(N_{11}, \dots, N_{nn}))$, причем оба эти многочлена принадлежат $A[Z]$; подставляя в них 0 вместо Z, получим $\det M = \det(D(M_{11}, \dots, M_{nn}))$.

Доказав эту лемму, разложим K-модуль V в прямую сумму K-модулей Ae_j $(1 \leqslant j \leqslant n)$; положим $u(e_j) = \sum_{k=1}^{n} c_{jk}e_k$. Для любого элемента $xe_j \in Ae_j$ (где $x \in A$) компонента элемента $u(xe_j)$ в Ae_k равна $xc_{jk}e_k$; отсюда следует, что матрица эндоморфизма u_k относительно базиса (a_ie_j) имеет вид квадратной таблицы (M_{jk}), где M_{jk} — матрица K-линейного отображения $xe_j \to xc_{jk}e_k$ модуля Ae_j в Ae_k относительно базисов $(a_ie_j)_{1 \leqslant i \leqslant m}$ и $(a_ie_k)_{1 \leqslant i \leqslant m}$ этих K-модулей (гл. II, § 6, n° 4). Матрица M_{jk}, очевидно, является также матрицей K-эндоморфизма алгебры $x \to xc_{jk}$ относительно базиса (a_i) алгебры A над K; отсюда следует, что матрицы M_{jk} *попарно перестановочны*, так что по лемме 2 $\det u_K = \det(D(M_{11}, \dots, M_{nn}))$. Однако $D(M_{11}, \dots, M_{nn})$ является, очевидно, матрицей K-эндоморфизма $x \to x \det(c_{jk})$ алгебры A относительно базиса (a_i); по определению, ее определитель равен тогда $N_{A/K}(\det(u))$, что доказывает вторую формулу (24). С другой стороны, $\mathrm{Tr}(u_K) = \sum_{j=1}^{n} \mathrm{Tr}(M_{jj}) =$

$= \sum_{j=1}^{n} \mathrm{Tr}_{A/K}(c_{jj}) = \mathrm{Tr}_{A/K}\left(\sum_{j=1}^{n} c_{jj}\right) = \mathrm{Tr}_{A/K}(\mathrm{Tr}(u))$, и тем самым предложение 7 полностью доказано.

Следствие. *Пусть K — коммутативное кольцо, A — коммутативная алгебра над K, имеющая над ним конечный базис, B — алгебра над A, имеющая над ней конечный базис. Тогда алгебра B имеет конечный базис над K и для всякого $x \in B$ выполняются равенства:*

$$\mathrm{Tr}_{B/K}(x) = \mathrm{Tr}_{A/K}(\mathrm{Tr}_{B/A}(x)), \qquad \mathrm{N}_{B/K}(x) = \mathrm{N}_{A/K}(\mathrm{N}_{B/A}(x)),$$
$$\mathrm{Pc}_{B/K}(x;\ X) = \mathrm{N}_{A[X]/K[X]}(\mathrm{Pc}_{B/A}(x;\ X)) \tag{26}$$

(«формулы транзитивности»).

Достаточно в предложении 7 заменить V на B, а u — на отображение $x \to xy$.

3. *Приведенные норма и след*

Пусть A — *простая алгебра* конечного ранга n^2 над своим центром K (§ 7, n° 4, следствие 3 теоремы 2), и L — ее нейтрализующее поле (§ 10, n° 5); по определению, алгебра $A_{(L)} = L \otimes_K A$ изоморфна алгебре матриц $\boldsymbol{M}_n(A)$. Для любого элемента $x \in A$ и любого L-изоморфизма h алгебры $L \otimes_K A$ на $\boldsymbol{M}_n(L)$ след, определитель и характеристический многочлен матрицы $h(1 \otimes x)$ не зависят от изоморфизма h (§ 10, n° 1, следствие теоремы 1). Покажем, что $\mathrm{Tr}(h(1 \otimes x))$ и $\det(h(1 \otimes x))$ — *элементы поля* K, $\mathrm{Pc}(h(1 \otimes x);\ X)$ — *элемент кольца* $K[X]$ *и все они не зависят* от рассматриваемого нейтрализующего поля L. Мы ограничимся доказательством этого утверждения для следа. Пусть f — K-изоморфизм поля L на некоторое расширение L' поля K; его единственным образом можно продолжить до K-изоморфизма алгебры $L \otimes_K A$ на $L' \otimes_K A$ и до K-изоморфизма алгебры $\boldsymbol{M}_n(L)$ на $\boldsymbol{M}_n(L')$; эти изоморфизмы также будем обозначать через f; $f \circ h \circ f^{-1}$ является L'-изоморфизмом h' алгебры $L' \otimes_K A$ на $\boldsymbol{M}_n(L')$, и для любого $x \in A$ имеем равенство $f(h(1 \otimes x)) = h'(1 \otimes x)$; следовательно, $\mathrm{Tr}(h'(1 \otimes x)) = f(\mathrm{Tr}(h(1 \otimes x)))$. Предположив сначала, что L — *поле Галуа* над K, и применив предыдущие рассуждения к K-автоморфизмам f поля L, убеж-

даемся, что в этом случае $\mathrm{Tr}\,(h\,(1\otimes x))$ принадлежит K. Пусть теперь L произвольно и N — расширение поля L (также нейтрализующее поле для A); алгебры $N\otimes_K A$ и $\boldsymbol{M}_n(N)$ можно канонически отождествить соответственно с $N\otimes_L (L\otimes_K A)$ и $N\otimes_L \boldsymbol{M}_n(L)$; тогда $h'=1\otimes h$ будет N-изоморфизмом алгебры $N\otimes_K A$ на $\boldsymbol{M}_n(N)$, таким, что при любом $x\in A$ матрицы $h\,(1\otimes x)$ и $h'\,(1\otimes x)$ имеют одни и те же элементы, а следовательно, *один и тот же след*. Окончательно наше утверждение следует из того, что поле Галуа над K, нейтрализующее для алгебры A, всегда существует (§ 10, n° 5, следствие предложения 7), и того, что два произвольных расширения поля K всегда K-изоморфны подполям одного и того же расширения поля K (гл. V, § 4, предложение 2, n° 2).

Элементы $\mathrm{Tr}\,(h\,(1\otimes x))$, $\det(h\,(1\otimes x))$ и $\mathrm{Pc}\,(h\,(1\otimes x))$ называются соответственно *приведенным следом*, *приведенной нормой* и *приведенным многочленом* элемента x над полем K и обозначаются $\mathrm{Trd}_{A/K}(x)$, $\mathrm{Nrd}_{A/K}(x)$ и $\mathrm{Pcrd}_{A/K}(x;\,X)$ (A и K опускаются, если это не может привести к недоразумению). Выполняются равенства:

$$\mathrm{Trd}\,(x+x')=\mathrm{Trd}\,(x)+\mathrm{Trd}\,(x'),\qquad \mathrm{Nrd}\,(xx')=\mathrm{Nrd}\,(x)\,\mathrm{Nrd}\,(x'),\tag{27}$$

$$\mathrm{Trd}\,(xx')=\mathrm{Trd}\,(x'x),\tag{28}$$

и если положить

$$\mathrm{Pcrd}\,(x;\;X)=X^n+b_{n-1}X^{n-1}+\ldots+b_0,$$

то

$$b_{n-1}=-\mathrm{Trd}\,(x),\qquad b_0=(-1)^n\,\mathrm{Nrd}\,(x).\tag{29}$$

Предложение 8. *Пусть A — простая алгебра конечного ранга n^2 над своим центром K. Для любого $x\in A$ имеем*

$$\mathrm{Tr}_{A/K}(x)=n\,\mathrm{Trd}_{A/K}(x),\qquad \mathrm{N}_{A/K}(x)=(\mathrm{Nrd}_{A/K}(x))^n,$$

$$\mathrm{Pc}_{A/K}(x;\;X)=(\mathrm{Pcrd}_{A/K}(x;\;X))^n.\tag{30}$$

Пусть L — нейтрализующее поле алгебры A, и S — простой $A_{(L)}$-модуль; матрица $h\,(1\otimes x)$ (в введенных выше обозначениях) является матрицей L-эндоморфизма $(1\otimes x)_S$ модуля S относительно подходящим образом выбранного базиса. С другой стороны, $A_{(L)}$ — прямая сумма n подмодулей, изоморфных S. Поэтому формулы (30) являются следствием формул (13) n° 2 и предложения 1 n° 1.

Предложение 9. *Пусть A — простая алгебра конечного ранга над своим центром K. Если элемент $a \in A$ удовлетворяет условию* $\mathrm{Trd}(ax) = 0$ *для всех* $x \in A$, *то* $a = 0$.

В самом деле, в предыдущих обозначениях, матрицы $h(1 \otimes ax) = h(1 \otimes a)\, h(1 \otimes x)$ при любом $x \in A$ имеют нулевой след; так как векторное L-пространство $L \otimes A$ порождается алгеброй A, то отсюда следует, что матрица $P = h(1 \otimes a)$ обладает свойством $\mathrm{Tr}(PX) = 0$ для любой матрицы $X \in \boldsymbol{M}_n(L)$, что влечет равенство $P = 0$ (гл. III, § 4, n° 5); следовательно, $a = 0$.

Предложение 10. *Пусть D — тело конечного ранга n^2 над своим центром K, x — такой элемент D, что $L = K(X)$ — максимальное подполе в D. Тогда минимальный многочлен элемента x над полем K равен* $\mathrm{Pc}_{D/K}(x; X)$.

В самом деле, из теоремы Гамильтона — Кэли (гл. VII, § 5, n° 3, следствие предложения 8) следует, что $\mathrm{Pc}_{D/K}(x; x) = 0$, и так как K — поле, то из предложения 8 следует, что и $\mathrm{Pcrd}_{D/K}(x; x) = 0$. Поскольку $\mathrm{Pcrd}_{D/K}(x; X)$ — унитарный многочлен степени n, то есть той же степени, что и минимальный многочлен элемента x над K (§ 10, n° 3, предложение 3), то тем самым утверждение доказано.

Предложение 11. *Пусть A — алгебра конечной размерности m над полем K, $(e_1, \ldots, e_m)$ — базис алгебры A над K. Существуют однородные многочлены* $\mathrm{Tr}(X_1, \ldots, X_m)$, $\mathrm{N}(X_1, \ldots, X_m)$, $\mathrm{Pc}(X_1, \ldots, X_m; X)$ *с коэффициентами из K степени соответственно* 1, m *и* m *такие, что для любого элемента $x = x_1e_1 + \ldots + x_me_m$ $(x_i \in K)$ алгебры A $\mathrm{Tr}_{A/K}(x) = \mathrm{Tr}(x_1, \ldots, x_m)$, $\mathrm{N}_{A/K}(x) = \mathrm{N}(x_1, \ldots, x_m)$, $\mathrm{Pc}_{A/K}(x) = \mathrm{Pc}(x_1, \ldots, x_m; X)$. Если, кроме того, алгебра A проста и $m = n^2$, то существуют однородные многочлены* $\mathrm{Trd}(X_1, \ldots, X_m)$, $\mathrm{Nrd}(X_1, \ldots, X_m)$, $\mathrm{Pcrd}(X_1, \ldots, X_m; X)$ *с коэффициентами из K степени соответственно* 1, n *и* n *такие, что* $\mathrm{Trd}_{A/K}(x) = \mathrm{Trd}(x_1, \ldots, x_m)$, $\mathrm{Nrd}_{A/K}(x) = \mathrm{Nrd}(x_1, \ldots, x_m)$, $\mathrm{Pcrd}_{A/K}(x) = \mathrm{Pcrd}(x_1, \ldots, x_m)$.

Положим $e_ie_j = \sum_k c_{ijk}e_k$ $(c_{ijk} \in K)$. Если $x = \sum_i x_ie_i$ $(x_i \in K)$, то матрица эндоморфизма $y \to xy$ относительно базиса (e_i) алгебры A равна $(\sum x_ic_{ijk})$. Следовательно, $\mathrm{Tr}_{A/K}(x) = \sum_{i,j} x_ic_{ijj}$,

$N_{A/K}(x) = \det(\sum_i x_i c_{ijk})$, $Pc_{A/K}(x;\ X) = \det(\delta_{jk}X - \sum_i x_i c_{ijk})$, что доказывает первое утверждение. Теперь будем предполагать, что алгебра A простая с центром K. Пусть L — ее нейтрализующее поле, являющееся *алгебраическим* расширением конечной степени поля K (§ 10, n° 5, следствие 3 предложения 7). Пусть h — изоморфизм алгебры $L \otimes A$ на $M_n(L)$ и $U_i = h(1 \otimes e_i)$; тогда $h(1 \otimes x) = \sum_i x_i U_i$, откуда $\mathrm{Trd}_{A/K}(x) = \mathrm{Tr}(\sum_i x_i U_i)$, $\mathrm{Nrd}_{A/K}(x) = \det(\sum_i x_i U_i)$, $\mathrm{Prd}_{A/K}(x;\ X) = \det(XI_n - \sum_i x_i U_i)$, откуда следует существование многочленов $\mathrm{Trd}(X_1, \ldots, X_m)$, $\mathrm{Nrd}(X_1, \ldots, X_m)$, $\mathrm{Prd}(X_1, \ldots, X_m; X)$, обладающих свойствами, указанными в формулировке предложения, но с коэффициентами *из поля* L.

Остается доказать, что коэффициенты этих многочленов лежат в K. Предположим сначала, что поле K *бесконечно*, и пусть $Q(X_1, \ldots, X_m) = \sum b_{\nu_1 \ldots \nu_m} X_1^{\nu_1} \ldots X_m^{\nu_m}$ — один из многочленов Trd, Nrd или некоторый коэффициент многочлена Prd, рассматриваемого как многочлен от X. Как мы видели в начале этого пункта, коэффициенты линейного уравнения относительно $t_{\nu_1 \ldots \nu_m}$

$$\sum t_{\nu_1 \ldots \nu_m} x_1^{\nu_1} \ldots x_m^{\nu_m} = Q(x_1, \ldots, x_m) \tag{31}$$

при любой системе $(x_1, \ldots, x_m)$ элементов из K лежат в поле K. С другой стороны, поскольку поле K бесконечно, то система уравнений (31) (где $x_1, \ldots, x_m$ пробегают K^m) имеет *единственное* решение $t_{\nu_1 \ldots \nu_m} = b_{\nu_1 \ldots \nu_m}$ (гл. IV, § 2, n° 5, предложение 8); отсюда следует, что элементы $b_{\nu_1 \ldots \nu_m}$ принадлежат K (гл. II, § 5, n° 3, теорема 1). В общем случае пусть Y — новая переменная, и рассмотрим алгебру $A_{(K(Y))} = K(Y) \otimes_K A$; эта алгебра простая, и ее центр равен $K(Y)$ (§ 7, n° 4, следствие 2 теоремы 2); элементы e_i $(1 \leqslant i \leqslant m)$ образуют базис алгебры $A_{(K(Y))}$ над $K(Y)$ (A отождествлена с подкольцом в $A_{(K(Y))}$). В поле $L(Y)$ подполя L и $K(Y)$ *линейно раздельны* над K (гл. V, § 5, n° 4, предложение 11); подалгебра, порожденная в $L(Y)$ полями L и $K(Y)$, имеет над $K(Y)$ конечный ранг и без делителей нуля, следовательно, является полем (гл. V, § 2, n° 1, следствие предложения 1); так как это поле содержит L и Y, то оно совпадает

с $L(Y)$, следовательно, $L(Y)$ отождествляется с тензорным произведением $K(Y) \otimes L$. Тогда тензорное произведение $A_{(L(Y))} = L(Y) \otimes_{K(Y)} A_{(K(Y))}$ отождествляется с $K(Y) \otimes_K A_{(L)}$ (см. § 10, n° 5), и поэтому поле $L(Y)$ — нейтрализующее для алгебры $A_{(K(Y))}$. Кроме того, отождествляя $\boldsymbol{M}_n(L(Y))$ с тензорным произведением $K(Y) \otimes_K \boldsymbol{M}_n(L)$, мы получим, что $h' = 1 \otimes h$ — изоморфизм алгебры $A_{(L(Y))}$ на $\boldsymbol{M}_n(L(Y))$. Отсюда следует, что для всякого элемента $y = \sum_i y_i e_i$ алгебры $A_{(K(Y))}$ $(y_i \in K(Y))$ выполняется равенство $\mathrm{Trd}_{A_{(K(Y))}/K(Y)}(y) = \mathrm{Tr}(\sum_i y_i U_i) = \mathrm{Trd}(y_1, \ldots, y_m)$, и такие же равенства справедливы для приведенной нормы и приведенного характеристического многочлена. Так как поле $K(Y)$ бесконечно, то заключаем отсюда, что коэффициенты многочленов Trd, Nrd и Pcrd лежат в $L \cap K(Y) = K$, что и заканчивает доказательство.

Заметим, что в первой части доказательства показано, что коэффициенты многочленов Tr, N и Pc являются многочленами от c_{ijk} с *целыми* коэффициентами, зависящими только от m.

Предложение 12. *Пусть A — алгебра над коммутативным кольцом K, конечной размерности над K. Для того чтобы элемент $x \in A$ был обратим в A, необходимо и достаточно, чтобы норма $\mathrm{N}_{A/K}(x)$ была обратима в K.*

Если x обратим, то $\mathrm{N}_{A/K}(x)\,\mathrm{N}_{A/K}(x^{-1}) = \mathrm{N}_{A/K}(1) = 1$, то есть условие необходимо. Обратно, если норма $\mathrm{N}_{A/K}(x)$ обратима в K, то K-эндоморфизм $y \to xy$ алгебры A биективен (гл. III, § 6, n° 5, теорема 2); существует, в частности, единственный элемент $x' \in A$ такой, что $xx' = 1$. Тогда $x(x'x - 1) = 0$, и, по предыдущему, отсюда следует $x'x = 1$, то есть x' — обратный элемент к x.

Следствие. *Пусть A — простая алгебра конечного ранга над своим центром K. Для того чтобы A была телом, необходимо и достаточно, чтобы из условия $x \neq 0$ в A следовало $\mathrm{Nrd}_{A/K}(x) \neq 0$.*

Это вытекает из предложения 12 и второй формулы (30).

Упражнения. 1) Пусть K — поле, имеющее не меньше трех элементов, A — алгебра над K с базисом, состоящим из 1 и элементов e_1, e_2 таких, что $e_1^2 = e_1$, $e_1e_2 = e_2$, $e_2e_1 = e_2^2 = 0$. Показать,

что существуют элементы $x \in A$ такие, что $\mathrm{Tr}_{A/K}(x) \neq \mathrm{Tr}_{A^0/K}(x)$ и $\mathrm{N}_{A/K}(x) \neq N_{A^0/K}(x)$.

2) Пусть A — алгебра конечного ранга n над полем K, $\mathrm{Pm}_{A/K}(x; X)$ — минимальный многочлен элемента $x \in A$ над K (§ 11, упражнение 1). Имеем равенство $\mathrm{Pm}_{A^0/K}(x; X) = \mathrm{Pm}_{A/K}(x; X)$.

а) Показать, что $\mathrm{Pm}_{A/K}(x; X)$ делит $\mathrm{Pc}_{A/K}(x; X)$ и $\mathrm{Pc}_{A/K}(x; X)$ делит $(\mathrm{Pm}_{A/K}(x; X))$.

б) При любом расширении L поля K и любом $x \in A$ выполняется равенство $\mathrm{Pm}_{A_{(L)}/L}(x \otimes 1; X) = \mathrm{Pm}_{A/K}(x; X)$.

в) Пусть $(a_i)_{1 \leqslant i \leqslant n}$ — базис алгебры A над K, Y_i $(1 \leqslant i \leqslant n)$ — n переменных; *главным многочленом* алгебры A относительно базиса (a_i) называется минимальный многочлен элемента $\sum_{i=1}^{n} Y_i a_i$ алгебры $A_{(K(Y_1, \ldots, Y_n))}$ над полем $K(Y_1, \ldots, Y_n)$; этот многочлен обозначается $P((a_i); X; Y_1, \ldots, Y_n)$ или просто $P(X; Y_1, \ldots, Y_n)$. Показать, что главный многочлен принадлежит $K[Y_1, \ldots, Y_n]$ (см. гл. VII, приложение, n° 3, предложение 5). Пусть (a'_i) — второй базис алгебры A над K, и $a_i = \sum_{j=1}^{n} \lambda_{ij} a'_j$; тогда $P((a_i); X; Y_1, \ldots, Y_n) = P((a'_i); X; Y'_1, \ldots, Y'_n)$, где $Y'_i = \sum_{k=1}^{n} \lambda_{ki} Y_k$. Для любого $x = \sum_{i=1}^{n} \xi_i a_i$ многочлен $P((a_i); X; \xi_1, \ldots, \xi_n)$ не зависит от рассматриваемого базиса (a_i) и называется *главным многочленом* элемента x над K; он делит $\mathrm{Pc}_{A/K}(x; X)$ и кратен $\mathrm{Pm}_{A/K}(x; X)$.

*3) Пусть A — простая алгебра конечного ранга над полем K, и Z — ее центр. Предположим, что Z является *сепарабельным* расширением поля K; положим $[A : Z] = n^2$, $[Z : K] = m$ и $[A : K] = r = mn^2$.

а) Показать, что для любого $x \in A$ степень многочлена $\mathrm{Pm}_{A/K}(x; X)$ не превосходит mn (используя третью формулу (30), заметить, что $[Z(x) : Z] \leqslant n$).

б) Показать, что главный многочлен алгебры A (относительно произвольного базиса A над K) имеет над полем $K(Y_1, \ldots, Y_r)$ степень mn и неприводим над этим полем. (Алгебра A изоморфна некоторой матричной алгебре $\boldsymbol{M}_q(D)$, где D — тело ранга s^2 над своим центром Z; отсюда следует, что $qs = n$. Пусть L — максимальное подполе в D, сепарабельное над Z. Заметить, что $L(Y_1, \ldots, Y_r)$ — подполе в $A_{(K(Y_1, \ldots, Y_r))}$ (см. § 7, упражнение 23), что у этого поля существуют сепарабельные расширения степени q (см. гл. V, при-

ложение I, n° 1, предложение 2) и что всякое такое поле изоморфно некоторой подалгебре в $\boldsymbol{M}_q(L(Y_1, \ldots, Y_r))$.

в) Пусть $Z = K$. Показать, что главный многочлен любого элемента $x \in A$ равен $\mathrm{Pcrd}_{A/K}(x; X)$ (использовать б)). Кроме того, группа Галуа (над полем $K(Y_1, \ldots, Y_r)$) главного многочлена алгебры A (относительно произвольного базиса) есть симметрическая группа $\mathfrak{S}_n$. (Рассматривая нейтрализующее поле алгебры A, свести доказательство к случаю $A = \boldsymbol{M}_n(K)$; рассуждая так же, как в б), показать, что коэффициенты главного многочлена алгебраически независимы над K.)

4) Пусть A — абсолютно полупростая алгебра над полем K, S_k $(1 \leqslant k \leqslant m)$ — различные классы простых A-модулей. Показать, что главный многочлен любого элемента $x \in A$ (упражнение 2в)) равен произведению многочленов $\mathrm{Pc}_{S_k/K}(x; X)$ $(1 \leqslant k \leqslant m)$.

5) Пусть A — алгебра конечного ранга над полем K и степень ее главного многочлена (относительно произвольного базиса A) равна m; *главным следом* элемента $x \in A$ называется коэффициент при $-X^{m-1}$ в главном многочлене элемента x; этот коэффициент обозначается $\mathrm{Trh}_{A/K}(x)$ или $\mathrm{Trh}(x)$.

а) Если элемент $x \in A$ нильпотентен, то $\mathrm{Tr}_{A/K}(x) = 0$ и для любого A-модуля M конечной размерности над K $\mathrm{Tr}_{M/K}(x) = 0$ (см. упражнения 2а) и 2в)). Вывести отсюда, что если $x \in A$ лежит в радикале алгебры A, то $\mathrm{Tr}_{M/K}(xy) = 0$ и $\mathrm{Trh}_{A/K}(xy) = 0$ для любого $y \in A$.

б) Пусть S_k $(1 \leqslant k \leqslant m)$ — различные классы простых A-модулей. Показать, что элемент $x \in A$ лежит в радикале алгебры A тогда и только тогда, когда $\mathrm{Tr}_{S_k/K}(xy) = 0$ для всех $y \in A$ и $1 \leqslant k \leqslant m$ (для доказательства достаточности применить следствие 2 теоремы 1 § 4, n° 2).

*6) Пусть K — поле характеристики 2, A — алгебра ранга 4 над K, определенная в упражнении 4б) § 11 (α и β — произвольные элементы K).

а) Показать, что минимальный многочлен над K любого элемента $x = x_0 + x_1 u + x_2 v + x_3 w$ алгебры A, не принадлежащего K, равен

$$X^2 + x_2 X + x_0^2 + x_0 x_2 + \beta x_2^2 + \alpha(x_1^2 + x_1 x_3 + \beta x_3^2).$$

Кроме того, $\mathrm{Pc}_{A/K}(x; X) = (\mathrm{Pm}_{A/K}(x; X))^2$. Вывести отсюда, что $\mathrm{Tr}_{A/K}(x) = 0$ для всякого $x \in A$.

б) Показать, что если $\alpha \neq 0$, то A — простая алгебра с центром K (использовать а) и упражнение 5а)). Если $\alpha = 0$, то радикал $\mathfrak{R}(A) = Ku + Kv$; если, кроме того, $\beta = \lambda + \lambda^2$ при некотором $\lambda \in K$, то $A/\mathfrak{R}(A)$ является прямой композицией двух полей, изоморфных K, а в противоположном случае $A/\mathfrak{R}(A)$ будет сепарабельным квадратичным расширением поля K.

в) Привести пример, в котором K — радикальное расширение степени 4 некоторого поля K_0, A — тело и главный многочлен A над K_0 имеет степень 4 (см. упражнение 3б)).

г) С помощью метода упражнения б) получить новым способом результаты об алгебрах кватернионов над полем характеристики $\neq 2$, сформулированные в упражнениях 4 и 6 гл. II, § 7.

*7) Пусть D — тело, σ — его автоморфизм. *Многочленами* (от одного переменного X) *над телом* D *относительно* σ называются элементы $f = f(X) = \sum_n \alpha_n X^n$ алгебры формальных степенных рядов, определенной в упражнении 10 гл. IV, § 5, в которых $\alpha_n = 0$ для всех n, кроме конечного числа; если $f \neq 0$, то наибольший индекс n такой, что $\alpha_n \neq 0$, называется *степенью* многочлена f и обозначается $\deg(f)$. Коэффициент α_m, где $m = \deg(f)$, называется старшим коэффициентом многочлена f; f называется унитарным, если его старший коэффициент равен 1. Обозначим через $D[X, \sigma]$ кольцо многочленов над телом D относительно автоморфизма σ. Напомним, что $Xa = a^\sigma X$ для любого $a \in D$.

а) Пусть f, g — элементы $A = D[X, \sigma]$ и $g \neq 0$. Показать, что существуют однозначно определенные элементы h_1, k_1 (соответственно h_2, k_2) кольца A такие, что $f = h_1 g + k_1$ (соответственно $f = g_2 h + k_2$) и $k_1 = 0$ или $\deg(k_1) < \deg(g)$ (соответственно $k_2 = 0$ или $\deg(k_2) < \deg(g)$).

б) Вывести из а), что всякий левый (соответственно правый) идеал в A моногенен. Показать, что если степени элементов f, g больше 0 и $Af + Ag = Ah$, $(Af) \cap (Ag) = Ak$, то $\deg(f) + \deg(g) = \deg(h) + \deg(k)$ (рассмотреть A-модуль Ah/Ak).

в) Всякое факторкольцо кольца A, отличное от A и от $\{0\}$, артиново. Пусть f — унитарный многочлен степени >0, и предположим, что $\mathfrak{a} = Af$ — двусторонний идеал в A; тогда $\mathfrak{a} = fA$. Для того чтобы $A/\mathfrak{a}$ было телом, необходимо и достаточно, чтобы многочлен f был *неприводим*, то есть не разлагался в произведение отличных от константы многочленов степеней $<\deg(f)$.

*8) Обозначения и предположения те же, что в упражнении 7.

а) Пусть $f(X) = X^n - a$, где $n > 1$, $a \in D$, $a \neq 0$. Идеал Af двусторонний тогда и только тогда, когда $a^\sigma = a$ и $x^{\sigma^n} = axa^{-1}$ для всякого $x \in D$.

б) Предположим, что n не делится на характеристику тела D, и центр D содержит примитивный корень n-й степени ω из 1 такой, что $\omega^\sigma = \omega$. Показать, что если неприводимый унитарный многочлен $g(X)$ является правым делителем многочлена $X^n - a$, то его степень g делит n, и f является произведением n/d многочленов степени d. (Пусть $g_k(X) = g(\omega^k X)$ и Ah — пересечение идеалов Ag_k $(0 \leqslant k \leqslant n-1)$; заметив, что тогда выполняется равенство $h(\omega X) = h(X)$, откуда $\deg(h) \geqslant n$, доказать, что Af совпадает с пересе-

чением Ah; затем воспользоваться упражнением 7б).) Если, кроме того, элемент $a \in D$ удовлетворяет условиям упражнения а), то факторкольцо A/Af полупросто и все его простые компоненты имеют одну и ту же длину (рассмотреть в A/A_f левые идеалы Ag_k/Af и воспользоваться упражнением 2в) § 3).

в) С этого момента будем предполагать, что элементы a и ω удовлетворяют условиям упражнения а) и б) и, кроме того, число n *простое*. Тогда:

α) если существует такой элемент $b \in D$, что автоморфизм σ совпадает с внутренним автоморфизмом $x \to bxb^{-1}$, и $a = b^n$, то факторкольцо $C=A/Af$ является прямой композицией n тел, изоморфных D;

β) если условия, указанные в α), не выполнены, но существует элемент $c \in D$ такой, что $a = c^{\sigma^{n-1}} c^{\sigma^{n-2}} \ldots c^{\sigma} c$, то C является простым кольцом длины n;

γ) если не существует такого элемента $c \in D$, что $a = c^{\sigma^{n-1}} c^{\sigma^{n-2}} \ldots c^{\sigma} c$, то C — тело (использовать б)).

Показать, что во всех этих случаях существует автоморфизм τ кольца C такой, что $\tau^k \neq 1$ при $k < n$ и $\tau^n = 1$, причем единственными инвариантными элементами кольца C при автоморфизме τ будут элементы тела D (отождествленного с его каноническим образом в C). В случаях β) и γ) D является в C *подтелом Галуа* (§ 10, упражнение 5). Частный случай — когда D — поле и когда $n = 2$.

г) Показать, что если σ является внутренним автоморфизмом $x \to c^{-1} xc$ тела D, то $a = c^{-n}\gamma$, где γ — элемент центра Z тела D, и кольцо C изоморфно тензорному произведению $D \otimes_Z B$, где $B = Z[X]/(h)$, $h(X) = X^n - \gamma$.

д) Показать, что если σ не является внутренним автоморфизмом тела D, то центр кольца C является подполем в центре Z тела D, состоящим из элементов Z, инвариантных относительно σ. Привести пример, где $n = 2$, σ — невнутренний автоморфизм тела D, и Z — центр кольца D (см. § 10, упражнение 10; в качестве K взять поле $K_0(Y)$ формальных степенных рядов над некоторым полем).

*9) Пусть K_0 — поле рациональных дробей $\boldsymbol{Q}(X)$, K — квадратичное расширение $K_0(\sqrt{-3})$, содержащее кубические корни из единицы j и j^2, D — циклическое расширение $K(\sqrt[3]{X})$, σ — образующий группы Галуа поля D над K. Рассмотрим алгебру C, определенную в упражнении 8, при $n = 3$, $a = 2$.

а) Показать, что C — тело ранга 9 над своим центром K. (Чтобы убедиться, что 2 не может быть представлено в виде $N_{D/K}(x)$, где $x \in D$, нужно лишь показать, что не может выполняться соотношение вида $P_1^3 + XP_2^3 + X^2P_3^3 - 3P_1P_2P_3X = 2P_4^3$, где P_i $(1 \leqslant i \leqslant 4)$ — независимые в совокупности многочлены с коэффициентами из поля $\boldsymbol{Q}(\sqrt{-3})$; для этого рассмотреть в многочленах P_i члены наименьшей степени.)

б) Показать, что единственный K_0-автоморфизм поля K, отличный от тождественного, не может быть продолжен до автоморфизма тела C (свести доказательство к случаю, когда такой автоморфизм τ удовлетворяет условию $\tau(D) = D$). Вывести отсюда, что K_0 не является подполем Галуа в C (§ 10, упражнение 5) и не существует K_0-автоморфизма тела C, имеющего порядок 2.

в) Пусть $\xi \in D$, $\xi^3 = X$ и $\eta \in C$, $\eta^3 = 2$, $\eta\xi = j\xi\eta$ (см. упражнение 8). Показать, что подполе $K(\zeta)$, где $\zeta = \eta + \eta^2 + \xi$, является в C максимальным подполем, но не подполем Галуа над K, и тогда подполя $K(\xi)$ и $K(\zeta)$ — поля Галуа над K.

*10) Пусть D — тело конечного ранга m^2 над своим центром K; обозначим через $D[X]$ кольцо многочленов над D относительно тождественного автоморфизма тела D (упражнение 7); это кольцо изоморфно $K[X] \otimes_K D$. Пусть элемент $x \in D$ не принадлежит K и $f(x) = X^n + \alpha_1 X^{n-1} + \ldots + \alpha_n$ — его минимальный многочлен над K.

а) Показать, что унитарный многочлен из кольца $D(X)$ степени $< n$ не может делиться справа на все многочлены вида $X - txt^{-1}$, где t пробегает D^* (рассмотреть среди унитарных многочленов, обладающих этим свойством, многочлен наименьшей степени и показать, что его коэффициенты должны лежать в K).

б) Пусть $u(X)$, $v(X)$, $w(X)$ — унитарные многочлены из кольца $D[X]$ такие, что $u(X) = v(X)\,w(X)$, и $X - x$ делит справа $u(X)$, но не делит справа $w(X)$, откуда следует $w(X) = r(X)(X - x) + t$, где $t \in D^*$. Показать, что $X - txt^{-1}$ — правый делитель многочлена $v(X)$.

в) Вывести из а) и б), что существует n элементов $t_i \in D$ $(1 \leqslant i \leqslant n)$ таких, что $f(X) = (X - t_1 x t_1^{-1}) \ldots (X - t_n x t_n^{-1})$ (заметить, что $f(X)$ делится справа на все многочлены $X - txt^{-1}$).

г) Вывести из в), что $\mathrm{Trd}_{D/K}(x)$ (соответственно $\mathrm{Nrd}_{D/K}(x)$) есть сумма (соответственно произведение) m элементов вида txt^{-1} (использовать следствие предложения 7).

11) Пусть A — алгебра конечного ранга над полем K. Предположим, что A наделена структурой совершенного порядка, удовлетворяющей аксиомам (МО) главы VI, § 1, n° 1 и (АО) главы VI, § 2, n° 1. Показать, что A — поле. (Показать сначала, что A не имеет делителей 0, то есть является телом, и имеет характеристику 0. Затем заметить, что если A некоммутативна, то в ней существуют не входящие в ее центр Z элементы $x \neq 0$ такие, что $\mathrm{Trd}_{A/Z}(x) = 0$; в заключение воспользоваться упражнением 10г).)

*12) Пусть D — тело кватернионов над полем Q рациональных чисел, соответствующее паре $(-1, -1)$.

а) Для того чтобы расширение K поля Q было нейтрализующим полем тела D, необходимо и достаточно, чтобы -1 была в поле K суммой двух квадратов (см. упражнение 8в)).

б) Пусть циклическое расширение N степени 2^n поля Q — нейтрализующее поле для D. Показать, что никакое его подполе, отличное от N, не будет нейтрализующим для D (заметить, что единственное подполе в N, имеющее степень 2^{n-1} над Q, является пересечением N и максимального упорядоченного поля, содержащего Q).

в) Пусть $k \geqslant 1$, и p — простой делитель числа $2^{2^k}+1$; пусть n — наибольшее целое число такое, что 2^n делит $p-1$; показать, что $n > k$ (заметить, что $2^{p-1} \equiv 1 \pmod{p}$). Пусть ω — примитивный корень степени p из единицы и $E = Q(\omega)$. Показать, что в поле E -1 является суммой двух квадратов. (Это утверждение равносильно тому, что в поле $F = E(\sqrt{-1})$ для некоторого $x \in F$ выполняется равенство $N_{F/E}(x)$.) Для доказательства существования такого элемента x заметить, что ω и $1+\omega^{2^h}$ являются нормами элементов поля F, и выразить -1 как произведение корня ω и некоторых элементов $1+\omega^{2^j}$, используя для этого тождество $\prod_{j=0}^{r-1}(1+x^{2^j}) = \sum_{h=0}^{2^r-1} x^h$.

г) Вывести из в), что если циклическое расширение N степени 2^n поля Q содержится в поле E, то N — нейтрализующее поле тела D. (В противном случае поле E не было бы нейтрализующим для D, так как $[E : N]$ нечетно; см. § 10, n° 5, следствие 1 предложения 7.)

*13) Пусть K — поле характеристики $\neq 2$, D_1, D_2 — алгебры кватернионов над K, соответствующие парам (α_1, β_1), (α_2, β_2). Тензорное произведение $D_1 \otimes_K D_2$ является телом тогда и только тогда, когда равенство

$$\alpha_1 x_1^2 + \beta_1 x_2^2 - \alpha_1\beta_1 x_3^2 = \alpha_2 y_1^2 + \beta_2 y_2^2 - \alpha_2\beta_2 y_3^2$$

влечет, что все x_i и y_i равны нулю. (Применяя упражнение 6 § 11, свести доказательство к случаю, когда D_1 — тело. Используя упражнение 8в), показать, что $D_1 \otimes D_2$ не является телом тогда и только тогда, когда в D_1 существуют такие перестановочные элементы x, y, что $\beta_2 = x^2 - \alpha_2 y^2$; если элементы x и y оба не принадлежат K, заметить, что $y \in K(x)$, и записать x в виде $s+t$, где $s \in K$, $\bar{t} = -t$.)

14) Пусть K_0 — поле характеристики $\neq 2$, (X_n) и (Y_n) — бесконечные последовательности переменных ($n \geqslant 1$), K — поле рациональных дробей $K_0(X_1, \ldots, X_n, \ldots, Y_1, \ldots, Y_n, \ldots)$. Обозначим через D_n, $n \geqslant 1$, тело кватернионов над K, соответствующее паре (X_n, Y_n).

а) Показать, что бесконечное тензорное произведение $D = \otimes_n D_n$ (гл. III, приложение I, n° 2) является телом с центром K и всякое его подтело, порожденное конечным подмножеством, имеет конечный ранг над K (использовать упражнение 8в)).

б) Пусть u — внутренний автоморфизм тела D; показать, что в N существует такое конечное подмножество H, что для любого $n \in H$ сужение автоморфизма u на D_n есть тождественный автоморфизм;

вывести отсюда, что тело D обладает несчетным множеством невнутренних K-автоморфизмов.

15) Используя следствие предложения 12 § 12, а также упражнение 8 гл. IV, § 2, показать, что всякое конечное тело коммутативно.

16) Пусть A — алгебра над полем K. *Спектром* произвольного элемента $a \in A$ называется множество элементов $\lambda \in K$ таких, что $\lambda - a$ необратим в K.

а) Пусть элемент a алгебраичен над K, и $f[X]$ — его минимальный многочлен над K. Показать, что спектром элемента a является множество корней многочлена f, принадлежащих K (использовать тождество Безу).

б) Пусть элемент a не алгебраичен над K и λ_i $(1 \leqslant i \leqslant n)$ — различные элементы поля K, не принадлежащие спектру элемента a; показать, что элементы $(\lambda_i - a)^{-1}$ линейно независимы над K (заметить, что все эти элементы принадлежат одной коммутативной подалгебре алгебры A).

в) Пусть поле K бесконечно и $\mathrm{Card}(K) > [A : K]$. Показать, что элементы радикала алгебры A алгебраичны над K (использовать б)); вывести отсюда, что $\mathfrak{R}(A)$ — нильидеал (см. § 11, упражнение 1).

§ 13. Линейные представления

1. *Линейные представления алгебр*

Определение 1. *Пусть K — коммутативное кольцо, A — алгебра над K, E — K-модуль. Линейным представлением алгебры A в E называется K-гомоморфизм алгебры A в алгебру $\mathscr{L}_K(E)$, переводящий единицу алгебры A в единицу $\mathscr{L}_K(E)$. Если модуль E имеет над K конечный базис, то размерность E над K называется размерностью или степенью представления.*

Пусть ϱ — линейное представление алгебры A в E. Аддитивный закон в E и отображение $(x, u) \to \varrho(x)u$ произведения $A \times E$ в E определяют на E структуру *левого A-модуля*; структура K-модуля на E, получающаяся из этой структуры A-модуля с помощью канонического гомоморфизма $\xi \to \xi \cdot 1$ поля K в A, представляет собой не что иное, как исходную структуру K-модуля E. Определенный таким образом K-модуль E называется *модулем представления* ϱ.

Обратно, пусть A — алгебра над K, E — левый A-модуль. С помощью канонического гомоморфизма поля K в A определим на E структуру K-модуля. Тогда отображение $x \to x_E$ будет K-гомоморфизмом алгебры A в алгебру $\mathscr{L}_K(E)$, то есть линейным

представлением ϱ алгебры A в K-модуль E; при этом модуль представления ϱ представляет собой не что иное, как данный A-модуль E; ϱ называется линейным представлением, ассоциированным с A-модулем E.

Таким образом, изучать линейные представления алгебры A — это то же самое, что изучать A-модули. Переведем некоторые определения относительно модулей на язык линейных представлений.

Ядром линейного представления называется аннулятор его модуля. Представление называется *точным*, если его модуль точный, другими словами, если его ядро равно нулю.

Линейное представление называется *простым* или *неприводимым*, если его модуль прост. Линейное представление называется *полупростым* или *вполне приводимым*, если его модуль полупрост.

Пусть ϱ, ϱ' — линейные представления алгебры A соответственно в E и E'. ϱ и ϱ' называются *подобными* или *изоморфными*, если их модули изоморфны, то есть существует такой K-изоморфизм φ модуля E на E', что $\varrho'(x) = \varphi \circ \varrho(x) \circ \varphi^{-1}$ для любого $x \in A$.

Пусть ϱ, ϱ' — линейные представления алгебры A. ϱ' называется *подпредставлением* (соответственно *факторпредставлением*) ϱ, если модуль M' представления ϱ' является подмодулем (соответственно фактормодулем) модуля M представления ϱ. Если ϱ' просто и ϱ полупросто, то говорят, что ϱ содержит ϱ' n раз, если изотипная компонента типа M' модуля M имеет длину n.

Прямой суммой семейства линейных представлений называется линейное представление, ассоциированное с прямой суммой их модулей. Прямая сумма представлений ϱ_i $(1 \leqslant i \leqslant n)$ обозначается через $\varrho_1 + \varrho_2 + \ldots + \varrho_n$.

Пусть ϱ — линейное представление алгебры A в K-модуль E, E^* — сопряженный к E модуль. Отображение $x \to {}^t\varrho(x)$ является представлением противоположной алгебры A^0 в E^* и называется *транспонированным представлением* для ϱ.

Пусть A — алгебра над K. Линейное представление алгебры A, ассоциированное с A-модулем A_s, называется *регулярным представлением* алгебры A. *Корегулярным представлением* алгебры A называется представление, транспонированное к регулярному представлению алгебры A^0.

З а м е ч а н и е. Пусть G — группа, K — коммутативное кольцо, E — K-модуль. *Линейным представлением* группы G в E называется гомоморфизм группы G в группу обратимых элементов кольца $\mathscr{L}_K(E)$.

Пусть $A = K^{(G)}$ — групповая алгебра группы G относительно кольца K (гл. II, § 7, n° 9). Существует единственный гомоморфизм K-модуля A в $\mathscr{L}_K(E)$, продолжающий заданное линейное представление группы G в E; этот гомоморфизм является гомоморфизмом алгебр и, следовательно, линейным представлением алгебры A в E. Обратно, для любого линейного представления ϱ алгебры A в E сужение ϱ на G является линейным представлением группы G в E. Следовательно, изучение линейных представлений группы G в E является иной формой изучения линейных представлений алгебры A в E, и понятия, относящиеся к представлениям алгебр, можно перенести на линейные представления групп.

2. *Матричные представления*

Пусть K — коммутативное кольцо и $n > 0$ — целое число. Кольцо эндоморфизмов K-модуля K^n канонически отождествляется с алгеброй $\boldsymbol{M}_n(K)$ квадратных матриц порядка n над кольцом K. Если A — алгебра над K, то линейное представление A в K^n является, следовательно, K-гомоморфизмом алгебры A в $\boldsymbol{M}_n(K)$ и, обратно, всякий K-гомоморфизм алгебры A в $\boldsymbol{M}_n(K)$ является линейным представлением A в K^n. Поэтому линейные представления алгебры A в K^n называются *матричными представлениями степени* n алгебры A. Если E — свободный K-модуль размерности n, то всякое линейное представление алгебры A в E подобно некоторому матричному представлению степени n.

Два матричных представления $x \to M_1(x)$ и $x \to M_2(x)$ подобны тогда и только тогда, когда они имеют одинаковую степень и существует такая обратимая матрица $P \in \boldsymbol{M}_n(K)$, что $M_2(x) = PM_1(x)P^{-1}$ для любого $x \in A$.

Далее до самого конца этого параграфа будет предполагаться, что K — поле.

Пусть E — A-модуль конечной размерности над K, ϱ — ассоциированное с ним представление. Пусть $E = E_p \supset E_{p-1} \supset \ldots \supset E_0 = \{0\}$ — некоторый композиционный ряд A-моду-

ля E; положим $q_j = \dim_K E_j$, $n_j = \dim_K E_j/E_{j-1} = q_j - q_{j-1}$, $1 \leqslant j \leqslant p$. Пусть $(e_i)_{1 \leqslant i \leqslant n}$ — такой базис модуля E над K, что $(e_1, e_2, \ldots, e_{q_j})$ — базис E_j над K, $1 \leqslant j \leqslant p$. Поскольку существует изоморфизм модуля K^n на E, отображающий канонический базис модуля K^n на (e_i), представление ϱ подобно матричному представлению вида

$$x \longrightarrow \begin{pmatrix} M_{11}(x) & M_{12}(x) & M_{13}(x) \ldots M_{1p}(x) \\ 0 & M_{22}(x) & M_{23}(x) \ldots M_{2p}(x) \\ 0 & 0 & M_{33}(x) \ldots M_{3p}(x) \\ \ldots & \ldots & \ldots \\ 0 & 0 & 0 \quad M_{pp}(x) \end{pmatrix},$$

где $M_{ij}(x)$ — матрица из n_i строк и n_j столбцов и все отображения $x \to M_{ij}(x)$ K-линейны. Отображения $x \to M_{ii}(x)$ являются матричными представлениями алгебры A, подобными линейным представлениям, ассоциированным с модулями E_i/E_{i-1}. Для того чтобы данный композиционный ряд был рядом Жордана — Гельдера, необходимо и достаточно, чтобы все представления $x \to M_{ii}(x)$ были неприводимыми. Тогда эти представления называются *неприводимыми компонентами* представления ϱ; ввиду теоремы Жордана — Гельдера (гл. I, § 6, n° 14, теорема 8) неприводимые компоненты определяются однозначно с точностью до порядка и подобия. Если для всякого i в E_i существует подмодуль (*над алгеброй* A), обладающий *дополнением* E_{i-1}, то представление ϱ подобно прямой сумме представлений $x \to M_{ii}(x)$ и, следовательно, подобно матричному представлению

$$x \longrightarrow \begin{pmatrix} M_{11}(x) & 0 \ldots 0 \\ 0 & M_{22}(x) \ldots 0 \\ \ldots & \ldots \\ 0 & 0 \quad M_{nn}(x) \end{pmatrix}.$$

3. *Коэффициенты представлений*

Пусть A — алгебра над полем K, ϱ — линейное представление A в векторном пространстве E над K. Пусть E^* — сопряженное к E векторное пространство. Для любых $u \in E$, $u' \in E^*$ через $\vartheta(u, u')$ обозначим K-линейную форму $x \to \langle \varrho(x)\, u, u' \rangle$ на

алгебре A. Ясно, что отображение $(u, u') \to \vartheta(u, u')$ произведения $E \times E^*$ в пространство A^*, сопряженное к векторному K-пространству A, билинейно. Линейные формы $\vartheta(u, u')$ (где u пробегает E, u' пробегает E^*) называются *коэффициентами* представления ϱ.

Если пространство E имеет над K конечный базис $(e_i)_{1 \leqslant i \leqslant n}$, и $(e'_i)_{1 \leqslant i \leqslant n}$ — сопряженный базис пространства E^*, то коэффициент $m_{ij}(x)$ матрицы эндоморфизма $\varrho(x)$ относительно базиса (e_i) равен $\vartheta(e_j, e'_i)(x)$. Этим и объясняется терминология.

Предложение 1. *Для любого $u' \in E^*$ отображение $u \to \vartheta(u, u')$ является A-гомоморфизмом пространства E в модуль A^* корегулярного представления алгебры A.*

В самом деле, по определению корегулярного представления, для любых $x, y \in A$ имеем

$$\vartheta(\varrho(y)u, u')(x) = \langle \varrho(x)(\varrho(y)u), u' \rangle = \langle \varrho(xy)u, u' \rangle = \vartheta(u, u')(xy) = (y\vartheta(u, u'))(x),$$

откуда $\vartheta(\varrho(y)u, u') = y\vartheta(u, u')$.

Следствие 1. *Пусть ϱ — неприводимое представление алгебры A, и $\vartheta(u, u')$ — отличный от нуля коэффициент представления ϱ. Тогда подмодуль, порожденный элементом $\vartheta(u, u')$ в A-модуле A^*, изоморфен модулю представления ϱ.*

Это утверждение немедленно следует из предложения 1 и леммы 2 § 4, n° 3.

Следствие 2. *Всякое неприводимое представление алгебры A подобно некоторому подпредставлению ее корегулярного представления.*

Пусть ϱ — линейное представление алгебры A, и $C(\varrho)$ — векторное подпространство в A^*, порожденное его коэффициентами. С помощью перенесения структуры легко убедиться, что для любых подобных представлений ϱ и ϱ' имеет место равенство $C(\varrho') = C(\varrho)$.

Предложение 2. *Пусть $\varrho_1, \ldots, \varrho_k$ — попарно не подобные неприводимые линейные представления алгебры A. Тогда сумма $C(\varrho_1) + C(\varrho_2) + \ldots + C(\varrho_k)$ в пространстве A^* прямая.*

В самом деле, предложение 1 и его следствие 1 показывают, что если E_{ρ_i} — модуль представления ρ_i, то $C(\rho_i)$ является изотипным типа E_{ρ_i} полупростым A-модулем; следовательно, предложение вытекает из предложения 9 § 3, n° 4.

Следствие. *Если два неприводимых представления алгебры A имеют одинаковый коэффициент, отличный от нуля, то они подобны.*

Пусть ρ_i $(1 \leqslant i \leqslant k)$ — линейное представление алгебры A в векторном пространстве E_i; известно, что пространство E^*, сопряженное к прямой сумме E пространств E_i, отождествляется с прямой суммой пространств E_i^*, каждое из которых отождествляется с подпространством в E^*, ортогональным к $\sum_{j \neq i} E_j$ (гл. II, § 4, n° 3, предложение 5); из определений немедленно следует, что если линейное представление ρ алгебры A является *прямой суммой* представлений ρ_i, то пространство $C(\rho)$ является *суммой* (вообще говоря, не прямой) подпространств $C(\rho_i)$.

Пусть A — *полупростая* алгебра над K; всякое ее линейное представление вполне приводимо (§ 5, n° 1, определение 1). Пусть A_i $(1 \leqslant i \leqslant r)$ — простые компоненты алгебры A; каждая алгебра A_i изоморфна кольцу матриц $\boldsymbol{M}_{n_i}(D_i)$ над телом D_i; тогда существует r неприводимых представлений ρ_i $(1 \leqslant i \leqslant r)$ алгебры A, попарно не подобных между собой и таких, что всякое неприводимое представление алгебры A подобно одному из ρ_i; кроме того, ядром ρ_i является сумма компонент A_j с индексами $j \neq i$ (§ 5, n° 3, предложение 11). В частности, регулярное представление алгебры A n_i раз содержит представление ρ_i, $1 \leqslant i \leqslant r$. С другой стороны, сопряженное пространство A^* отождествляется с прямой суммой сопряженных пространств A_i^*. Покажем, что $C(\rho_i) = A_i^*$ $(1 \leqslant i \leqslant r)$. Очевидно, можно ограничиться тем, что рассматривать ρ_i как линейное представление алгебры A_i; тогда, по предыдущему, для *любого* линейного представления ρ алгебры A_i выполняется равенство $C(\rho) = C(\rho_i)$; но если ρ — регулярное представление алгебры A_i, то всякая линейная форма $u' \in A_i^*$ является его коэффициентом — это следует из того, что она может быть записана в виде $x \to \langle x \cdot 1, u' \rangle$.

Предположим дополнительно, что полупростая алгебра A имеет *конечный* ранг над полем K; тогда, если $[A_i : K] = m_i$, то

представление ϱ_i имеет конечный ранг m_i/n_i. Кроме того, A-модуль A_i^* аннулируется алгебрами A_j с индексами $j \neq i$ и $[A_i^* : K] = m_i$, поэтому A_i^* изоморфен A-модулю A_i, откуда следует, что регулярное и корегулярное представления алгебры A *подобны* (см. упражнение 1).

4. *Расширение основного поля линейного представления*

Пусть A — алгебра над полем K, ϱ — линейное представление алгебры A, E — A-модуль, ассоциированный с ϱ. Для любого (коммутативного) расширения L поля K тензорное произведение $E_{(L)} = E \otimes_K L$ является модулем над алгеброй $A_{(L)} = A \otimes_K L$ (§ 7, n° 1); линейное представление алгебры $A_{(L)}$, ассоциированное с модулем $E_{(L)}$, будем называть полученным из представления ϱ *расширением поля скаляров до* L и обозначать через $\varrho_{(L)}$. Если ϱ — матричное представление, то $\varrho_{(L)}$ — матричное представление той же самой степени, и для любого $x \in A$ матрица, соответствующая элементу $x \otimes 1$ при представлении $\varrho_{(L)}$, совпадает с матрицей, соответствующей элементу x при представлении ϱ.

Предложение 3. *Если представление* $\varrho_{(L)}$ *неприводимо* (соответственно *вполне приводимо*), *то представление* ϱ *неприводимо* (соответственно *вполне приводимо*).

Это немедленно следует из теоремы 2 § 7, n° 4.

Предложение 4. *Если* ϱ *— вполне приводимое представление конечной степени, и* L *— сепарабельное расширение поля* K, *то представление* $\varrho_{(L)}$ *вполне приводимо.*

Очевидно, можно ограничиться случаем, когда представление ϱ неприводимо. Тело D — коммутант модуля представления ϱ — имеет тогда конечный ранг над K, так что алгебра $D \otimes_K L$ полупроста (§ 7, n° 6, следствие 4 теоремы 3) и, следовательно, модуль $E \otimes_K L$ полупрост (§ 7, n° 4, теорема 2); отсюда и следует доказываемое утверждение.

Линейное представление ϱ алгебры A называется *абсолютно полупростым*, если при любом расширении L поля K *представление* $\varrho_{(L)}$ *полупросто*; если представление ϱ имеет конечную степень,

то для этого достаточно, чтобы было полупростым представление $\varrho_{(\Omega)}$, где Ω — алгебраическое замыкание поля K (§ 7, n° 5, предложения 5 и 7). Для того чтобы линейное представление конечной степени ϱ было абсолютно полупростым, необходимо и достаточно, чтобы ϱ было полупростым и центры коммутантов простых подмодулей модуля представления ϱ были сепарабельны над K (§ 7, n° 5, предложения 6 и 7).

Линейное представление ϱ алгебры A называется *абсолютно простым* или *абсолютно неприводимым*, если при любом расширении L поля K представление $\varrho_{(L)}$ неприводимо.

Предложение 5. *Для того чтобы линейное представление конечной степени ϱ было абсолютно неприводимым, необходимо и достаточно, чтобы $\varrho(A) = \mathscr{L}(E)$.*

Достаточность условия очевидна (§ 3, n° 1, пример 2). Обратно, пусть $\varrho(A) \neq \mathscr{L}(E)$; рассматривая в пространстве $\mathscr{L}(E)$ над полем K дополнительное к $\varrho(A)$ подпространство, можно убедиться, что $(\varrho(A))_{(L)} \neq (\mathscr{L}(E))_{(L)}$ при любом расширении L поля K; но взяв в качестве L алгебраически замкнутое расширение поля K, ввиду теоремы Бернсайда (§ 4, n° 3, следствие 1 предложения 2) получим противоречие с тем, что представление $\varrho_{(L)}$ просто.

Следствие. *Для того чтобы вполне приводимое линейное представление конечной степени ϱ было абсолютно неприводимым, необходимо и достаточно, чтобы коммутант модуля представления ϱ совпадал с K.*

Ввиду предложения 5 (гл. II, § 2, n° 5, следствие 1 предложения 5) условие необходимо. Обратно, если коммутант модуля M представления ϱ равен K, то его бикоммутант равен $\mathscr{L}(E)$, и поскольку M — полупростой модуль конечного типа, то $\varrho(A) = \mathscr{L}(E)$ (§ 4, n° 2, следствие 1 теоремы 1); следовательно, представление ϱ абсолютно неприводимо (предложение 5).

Пусть ϱ — абсолютно неприводимое матричное представление степени n; тогда образом центра алгебры A является множество матриц вида λI_n, где $\lambda \in K$. Следовательно, если алгебра A коммутативна, то все ее неприводимые представления имеют *степень* 1 (иными словами, являются ненулевыми гомоморфизмами алгебры A в K).

5. *Норма и след относительно представления*

Пусть A — алгебра над полем K, ϱ — линейное представление алгебры A конечной степени n, E — модуль представления ϱ. *Характеристическим многочленом* (соответственно *нормой*, *следом*) произвольного *элемента* $x \in A$ *относительно представления* ϱ называется характеристический многочлен (соответственно норма, след) элемента x относительно модуля E; этот элемент обозначается через $\mathrm{Pc}_\varrho(x; X)$ (соответственно $\mathrm{N}_\varrho(x)$, $\mathrm{Tr}_\varrho(x)$). Мы предоставляем читателю перенесение на эти понятия свойств, установленных в § 12, n° 1.

Упражнения. 1) Пусть A — алгебра, определенная в упражнении 1 § 12. Показать, что ее регулярное и корегулярное представления не подобны и у корегулярного представления имеются такие подпредставления, которые не подобны ни одному подпредставлению и ни одному факторпредставлению регулярного представления. Показать, что существует неприводимое представление алгебры A, не подобное никакому подпредставлению регулярного представления алгебры A.

2) Пусть A — алгебра, определенная в упражнении 13 § 5. Показать, что не существует неприводимого представления алгебры A, подобного некоторому подпредставлению ее регулярного представления.

3) Пусть A — алгебра конечного ранга над полем K и все ее нильпотентные элементы лежат в ее центре. Показать, что всякое неприводимое представление алгебры A подобно некоторому подпредставлению ее регулярного представления (см. § 6, упражнение 23).

4) Пусть A — алгебра над полем K, и A^* — сопряженное векторное пространство к A; рассмотрим A^* как левый A-модуль. Пусть $\mathfrak{S}$ — множество классов простых A-модулей, и для любого $\lambda \in \mathfrak{S}$ пусть ϱ_λ — представление, ассоциированное с A-модулем λ.

а) Показать, что векторное подпространство V алгебры A является правым идеалом в A тогда и только тогда, когда V — подпространство, ортогональное к некоторому подмодулю V' модуля A^*; подпространство $V'' \supset V'$ в A^*, ортогональное к V, является тогда подмодулем в A^*.

б) Показать, что подпространство коэффициентов $C(\varrho_\lambda)$ есть сумма простых подмодулей типа λ модуля A^* и что подпространство в A, ортогональное к сумме всех $C(\varrho_\lambda)$, есть радикал алгебры A.

в) Показать, что подпространство в A^*, ортогональное к правому цоколю алгебры A (§ 5, упражнение 9), является радикалом A-модуля A^*. Вывести отсюда, что A-модуль A^* полупрост тогда и только тогда, когда полупроста алгебра A.

*5) а) В обозначениях и предположениях упражнения 21 § 6, пусть M — левый A-модуль конечной длины и множество его подмодулей, отличных от M, имеет наибольший элемент N, причем фактормодуль M/N изоморфен $\overline{Ae}$. Показать, что M изоморфен фактормодулю модуля Ae (заметить, что $eM \neq \{0\}$, и вывести отсюда, что если $x \in eM$ не лежит в N, то $Ax = M$).

б) Предположим дополнительно, что алгебра A *инволютивна* (§ 2, упражнение 11) и разложена в прямую сумму неразложимых левых идеалов

$$Ae_{k,i} \quad (1 \leqslant k \leqslant r, \quad 1 \leqslant i \leqslant f(k) \text{ для любого } k),$$

где $e_{k,i}$ — ортогональные идемпотенты, идеалы $Ae_{k,i}$, соответствующие одному значению k, попарно изоморфны, и каждый из модулей

$$\sum_{i=1}^{f(h)} \overline{Ae_k}$$

является изотипной компонентой фактормодуля $A/\mathfrak{R}(A)$ (§ 6, упражнения 19г) и 21а)). Показать, что существует такая перестановка π отрезка $[1, r]$, что каждый правый идеал $e_{k,i}A$ содержит единственный минимальный правый идеал, изоморфный (как A-модуль) $\overline{e_{\pi(k),1}A}$ (заметить, что если e — идемпотент, то правый аннулятор идеала Ae равен $(1 - e)A$). Вывести отсюда, что левый цоколь S алгебры A содержится в ее правом цоколе T (показать, что правые идеалы $e_{k,i}S$ минимальны, установив для этого, что каждый из них является аннулятором некоторого максимального левого идеала; см. § 6, упражнение 33). В заключение вывести, что $S = T$ и что всякий левый идеал $Ae_{\pi(k),i}$ содержит единственный минимальный левый идеал, изоморфный (как A-модуль) $\overline{Ae_{k,1}}$. Показать, что, обратно, если всякий идеал $Ae_{k,i}$ и всякий идеал $e_{k,i}A$ содержат *единственный* минимальный идеал, то алгебра A инволютивна. (Используя упражнение 21 § 6, показать, что каждое основание левого цоколя S является минимальным двусторонним идеалом, вывести отсюда, что $S \subset T$ и затем $S = T$; доказать, наконец, что выполнены условия α_s) и α_d) упражнения 11 § 2.)

в) Пусть A — алгебра конечного ранга над полем K. Показать, что если A — инволютивное кольцо, то ее линейное представление, ассоциированное с левым A-модулем $Ae_{\pi(k),1}$, подобно транспонированному линейному представлению алгебры A^0, ассоциированному с правым A-модулем $e_{k,1}A$. (Пусть U_k — подпространство в A^*, ортогональное к $(1 - e_{k,1}A)$; используя а), показать, что левый A-модуль U_k (упражнение 4а)) изоморфен фактормодулю модуля $Ae_{\pi(k),1}$ и, следовательно (§ 2, упражнение 11) длина модуля $Ae_{k,1}$ не прево-

сходит длины $Ae_{\pi(k),i}$. Вывести отсюда, что эти длины должны быть равны и поэтому подпространство U_k изоморфно $Ae_{\pi(k),1}$.) Доказать обратное утверждение (использовать б) и упражнение 4а)).

6) а) Показать, что если (в обозначениях и предположениях упражнения 5б)) A — *фробениусово* кольцо (§ 4, упражнение 10), то для любого k ($1 \leqslant k \leqslant r$) справедливо равенство $f(\pi(k)) = f(k)$. Доказать обратное утверждение.

б) Показать, что алгебра A конечного ранга над полем K фробениусова тогда и только тогда, когда ее регулярное представление подобно ее корегулярному представлению (использовать упражнение 5в), а также теорему 1 § 2, n° 2).

ПРИЛОЖЕНИЕ

АЛГЕБРЫ БЕЗ ЕДИНИЦЫ

Во всем этом приложении K — поле, A — алгебра над полем K, с единицей или без единицы. Напомним, что, по определению, идеал (левый, правый или двусторонний) алгебры A устойчив относительно операторов из поля K, то есть является векторным подпространством над K (гл. I, § 8, n° 5, определение 5).

1. Регулярные идеалы

Определим на множестве $\widetilde{A} = K \times A$ следующие законы композиции:

$$(\lambda,\ a)+(\mu,\ b)=(\lambda+\mu,\ a+b),$$
$$(\lambda,\ a)(\mu,\ b)=(\lambda\mu,\ ab+\mu a+\lambda b),$$
$$\lambda(\mu,\ a)=(\lambda\mu,\ \lambda a).$$

Легко проверяется, что множество $\widetilde{A}$, наделенное этими законами композиции, является *алгеброй над полем* K. Элемент $e = (\varepsilon, 0)$, где ε — единица поля K, будет единичным элементом алгебры $\widetilde{A}$. Множество $\{0\} \times A$ является в $\widetilde{A}$ двусторонним идеалом, и отображение $x \to (0, x)$ является изоморфизмом алгебры A на подалгебру $\{0\} \times A$, посредством которого эти алгебры отождествляются. $\widetilde{A}$ называют *алгеброй, полученной из A присоединением единицы.*

Предложение 1. а) *Пусть $\widetilde{\mathfrak{a}}$ — левый идеал алгебры $\widetilde{A}$, не содержащийся в A. Существует такой элемент $u \in A$, что $u - e \in \widetilde{\mathfrak{a}}$; левый идеал $\mathfrak{a} = A \cap \widetilde{\mathfrak{a}}$ алгебры A обладает свойством хи — $x \in \mathfrak{a}$ для любого $x \in A$, и $\widetilde{\mathfrak{a}} = \mathfrak{a} + K(u - e)$.*

б) *Пусть* $\mathfrak{a}$ *— левый идеал алгебры* A *и элемент* $u \in A$ *таков, что* $xu - x \in \mathfrak{a}$ *для любого* $x \in A$. *Пусть* $\tilde{\mathfrak{a}} = \mathfrak{a} + K(u - e)$. *Тогда* $\tilde{\mathfrak{a}}$ *— левый идеал в* A, *не содержащийся в* A, *и* $\mathfrak{a} = A \cap \tilde{\mathfrak{a}}$.

а) Так как, по предположению, $\tilde{\mathfrak{a}}$ не содержится в A, то, по определению A, в $\tilde{\mathfrak{a}}$ существует элемент вида $v - \lambda e$, где $v \in A$ и $\lambda \in K$, $\lambda \neq 0$. Положив $u = \lambda^{-1} v$, убедимся, что $u - e \in \tilde{\mathfrak{a}}$. Ясно, что $\tilde{\mathfrak{a}} = \mathfrak{a} + K(u - e)$; кроме того, если $x \in A$, то $xu - x = x(u - e) \in \tilde{\mathfrak{a}}$, так что $xu - x \in \tilde{\mathfrak{a}}$.

б) По предположению, $x(u - e) = xu - x \in \mathfrak{a}$ для любого $x \in A$, то есть $A\tilde{\mathfrak{a}} = A\mathfrak{a} + A(u - e) \subset \tilde{\mathfrak{a}}$; так как $\tilde{\mathfrak{a}}$ является векторным пространством над K, то $\tilde{\mathfrak{a}}$ будет левым идеалом в $\tilde{A}$, не содержащимся, очевидно, в A, и при этом $\mathfrak{a} = A \cap \tilde{\mathfrak{a}}$.

Определение 1. *Пусть* $\mathfrak{a}$ *— левый* (соответственно *правый*) *идеал алгебры* A. *Элемент* $u \in A$ *такой, что* $xu - x \in \mathfrak{a}$ (соответственно $ux - x \in \mathfrak{a}$) *при любом* $x \in A$, *называется правой* (соответственно *левой*) *единицей по модулю* $\mathfrak{a}$. *Идеал* $\mathfrak{a}$ *называется регулярным, если существует правая* (соответственно *левая*) *единица по модулю* $\mathfrak{a}$.

Если алгебра A имеет единицу 1, то 1 является правой (соответственно левой) единицей по модулю любого левого (соответственно правого) идеала алгебры A.

Пусть $\mathfrak{a}$ — регулярный левый идеал алгебры A, u — правая единица по модулю $\mathfrak{a}$. Если $\mathfrak{b} \supset \mathfrak{a}$ — произвольный левый идеал алгебры A, то u — правая единица по модулю $\mathfrak{b}$, и следовательно, идеал $\mathfrak{b}$ регулярен. Для любого левого идеала алгебры A утверждение, что он максимален и регулярен, равносильно тому, что он является максимальным элементом в множестве регулярных идеалов, отличных от A. С другой стороны, если $\mathfrak{a} \neq A$, то $u \in \mathfrak{a}$. Применяя теорему Цорна к индуктивному множеству левых идеалов, содержащих $\mathfrak{a}$ и отличных от A, получаем следующий результат.

Предложение 2. *Всякий регулярный левый* (соответственно *правый*) *идеал, отличный от* A, *содержится в максимальном регулярном левом* (соответственно *правом*) *идеале*.

Предложение 3. *Предположим, что алгебра A* коммутативна. *Пусть $\mathfrak{a}$ — идеал в A. Для того чтобы идеал $\mathfrak{a}$ был максимальным регулярным идеалом, необходимо и достаточно, чтобы факторалгебра $A/\mathfrak{a}$ была полем.*

В самом деле, пусть $x \to \dot{x}$ — каноническое отображение алгебры A на $A/\mathfrak{a}$. Идеалы алгебры $A/\mathfrak{a}$ являются образами при этом отображении идеалов алгебры A, содержащих $\mathfrak{a}$. Следовательно, если $A/\mathfrak{a}$ — поле, то идеал $\mathfrak{a}$ максимален; с другой стороны, всякий элемент алгебры A, образ которого в $A/\mathfrak{a}$ равен единице поля $A/\mathfrak{a}$, является единицей по модулю $\mathfrak{a}$. Обратно, пусть $\mathfrak{a}$ — максимальный регулярный идеал и u — единица по модулю $\mathfrak{a}$. Тогда $\dot{u}$ — единица кольца $A/\mathfrak{a}$. Кроме того, единственными идеалами в $A/\mathfrak{a}$ являются $A/\mathfrak{a}$ и $\{0\}$, то есть $A/\mathfrak{a}$ — поле (гл. I, § 9, n° 3, предложение 3).

Замечание. Можно определить регулярные идеалы и в предположении, что K — коммутативное кольцо с единицей и A — алгебра над K. Предложения 2 и 3 остаются в этом случае в силе, так как условие, что K — поле, в них не используется.

Пусть $\mathfrak{I}$ — множество левых идеалов алгебры $\tilde{A}$, не содержащихся в A. В силу предложения 1 отображение $\tilde{\mathfrak{a}} \to \tilde{\mathfrak{a}} \cap A$ множества $\mathfrak{I}$ во множество регулярных левых идеалов алгебры A *сюръективно*, но, вообще говоря, не инъективно (упражнение 4). Однако имеет место

Предложение 4. *Пусть $\tilde{\mathfrak{a}}$ — максимальный левый идеал в $\tilde{A}$ и $\mathfrak{a} = \tilde{\mathfrak{a}} \cap A$. Отображение $\tilde{\mathfrak{a}} \to \mathfrak{a}$ является биекцией множества максимальных левых идеалов алгебры $\tilde{A}$, отличных от A, на множество максимальных регулярных левых идеалов алгебры A.*

Пусть $\tilde{\mathfrak{a}}$ — левый идеал в $\tilde{A}$, не содержащийся в A, $\mathfrak{a} = \tilde{\mathfrak{a}} \cap A$ и u — правая единица по модулю $\mathfrak{a}$. Предположим, что $\mathfrak{a}$ содержится в левом идеале $\mathfrak{b}$ алгебры A, отличном от $\mathfrak{a}$ и A. Тогда u является также правой единицей по модулю $\mathfrak{b}$ и $\tilde{\mathfrak{b}} = \mathfrak{b} + K(u - e)$ — левый идеал алгебры $\tilde{A}$, содержащий $\tilde{\mathfrak{a}}$ (предложение 1) и отличный от $\tilde{A}$ и от $\tilde{\mathfrak{a}}$.

Пусть теперь $\tilde{\mathfrak{a}}$ содержится в левом идеале $\tilde{\mathfrak{b}}$ алгебры $\tilde{A}$, отличном от $\tilde{A}$ и от $\tilde{\mathfrak{a}}$. Так как $\tilde{\mathfrak{a}} \cap A$ и $\tilde{\mathfrak{b}} \cap A$ имеют соответ-

ственно в $\tilde{\mathfrak{a}}$ и $\tilde{\mathfrak{b}}$ факторразмерность 1, то из условия $\tilde{\mathfrak{a}} \cap A = \tilde{\mathfrak{b}} \cap A$ следует $\tilde{\mathfrak{a}} = \tilde{\mathfrak{b}}$; поэтому $\tilde{\mathfrak{a}} = \mathfrak{a} + K(u - e)$; кроме того, $\tilde{\mathfrak{b}} \cap A \neq A$, так как иначе выполнялось бы равенство $\tilde{\mathfrak{b}} = A$, так как $\tilde{\mathfrak{b}}$ не содержится в A.

Это показывает, что $\tilde{\mathfrak{a}} \to \tilde{\mathfrak{a}} \cap A$ — *сюръективное* отображение множества $\mathfrak{M}$ максимальных левых идеалов алгебры $\tilde{A}$, отличных от A, на множество максимальных регулярных идеалов алгебры A. Остается показать, что если $\tilde{\mathfrak{a}}$ и $\tilde{\mathfrak{b}}$ — элементы множества $\mathfrak{M}$, то равенство $\tilde{\mathfrak{a}} \cap A = \tilde{\mathfrak{b}} \cap A$ влечет $\tilde{\mathfrak{a}} = \tilde{\mathfrak{b}}$. Однако по предложению 1 имеем равенство $\tilde{\mathfrak{a}} = \mathfrak{a} + K(u - e)$, где u — правая единица по модулю $\mathfrak{a}$. Достаточно, следовательно, доказать следующую лемму:

Лемма 1. *Пусть* $\mathfrak{a}$ — *максимальный регулярный идеал алгебры* A, *и* u *и* v — *две правые единицы по модулю* $\mathfrak{a}$. *Тогда* $u - v \in \mathfrak{a}$.

В самом деле, для любого $x \in A$ выполняется равенство $x(u - v) = (xu - x) - (xv - x) \in \mathfrak{a}$, и поэтому $\mathfrak{a} + K(u - v)$ является левым идеалом в алгебре A. Если $u - v \overline{\in} \mathfrak{a}$, то $\mathfrak{a} + K(u - v) = A$, откуда $u = \lambda v + w$, где $\lambda \in K$, $\lambda \neq 1$ и $w \in \mathfrak{a}$; отсюда $x(\lambda - 1)\, v \in \mathfrak{a}$ при любом $x \in A$, то есть $xv \in \mathfrak{a}$, и поскольку, по предположению, $xv - x \in \mathfrak{a}$, то $x \in \mathfrak{a}$; следовательно, $\mathfrak{a} = A$, что неверно.

Применяя предложения 1 и 4 к кольцу A^0, можно получить аналогичные предложения для правых идеалов.

2. *Простые модули*

Левым модулем над алгеброй A называется векторное пространство E над полем K, наделенное такой структурой левого модуля над *кольцом* A, что $a(\lambda x) = \lambda(ax) = (\lambda a)\, x$ для всех $\lambda \in K$, $a \in A$ и $x \in E$. Подмножество F модуля E является модулем над алгеброй A тогда и только тогда, когда F — векторное подпространство в E и модуль над кольцом A; подмножество F называют тогда *подмодулем* модуля E над алгеброй A. Модуль E над алгеброй A называется простым, если $E \neq \{0\}$ и единственными его подмодулями над алгеброй A являются E и $\{0\}$.

Пусть E — левый модуль над алгеброй A. Для любых $\lambda \in K$, $a \in A$, $x \in E$ положим $(\lambda, a)\, x = \lambda x + ax$; легко проверяется, что этот закон внешней композиции и сложение определяют на E структуру *унитарного* $\tilde{A}$-модуля. Если сузить кольцо операторов этого $\tilde{A}$-модуля до A (соответственно до K, отождествленного с $K \times \{0\}$), то мы возвращаемся к заданной на E структуре модуля над кольцом A (соответственно структуре векторного пространства над K). Определенный таким образом $\tilde{A}$-модуль называется *ассоциированным* с модулем E над алгеброй A.

Обратно, пусть E — унитарный $\tilde{A}$-модуль. Рассмотренные сужения определяют на E структуру модуля над алгеброй A и структуру векторного пространства над K, причем ассоциированным $\tilde{A}$-модулем будет исходный $\tilde{A}$-модуль E. Таким образом, утверждения, что модуль E над алгеброй A прост и что ассоциированный $\tilde{A}$-модуль прост, эквивалентны.

Замечание. Пусть алгебра A имеет единицу и E — унитарный модуль над алгеброй A. Структура векторного K-пространства на E получается сужением кольца операторов A до K, отождествленного с подполем $K \cdot 1$ кольца A. Подмодули модуля E над алгеброй A совпадают, таким образом, в этом случае с подмодулями модуля E над кольцом A. Следовательно, утверждать, что E — простой (унитарный) модуль над алгеброй A,— это значит утверждать, что E — простой (унитарный) модуль над кольцом A.

Пусть $\mathfrak{a}$ — регулярный левый идеал алгебры A. Канонический образ z правой единицы по модулю $\mathfrak{a}$ в модуле $E = A/\mathfrak{a}$ над алгеброй A удовлетворяет условию $E = Az$, и $\mathfrak{a}$ является аннулятором элемента z. Обратно, пусть M — модуль над алгеброй A, $z \in M$ — такой элемент, что $M = Az$, и $\mathfrak{a}$ — левый идеал, аннулятор элемента z. Пусть $u \in A$ и $uz = z$. Для любого $x \in A$ имеем $(xu - x)\, z = 0$, то есть $xu - x \in \mathfrak{a}$, откуда следует, что идеал $\mathfrak{a}$ регулярен, и u — правая единица по модулю $\mathfrak{a}$.

3. *Радикал*

Предложение 5. *Пусть $\mathfrak{R}_1$ — пересечение аннуляторов простых левых модулей над алгеброй A, $\mathfrak{R}_2$ — пересечение максимальных левых идеалов алгебры A, $\mathfrak{R}_3$ — радикал кольца A. Все эти множества представляют собой один и тот же двусторонний идеал*

алгебры A, не меняющийся при замене A на противоположную алгебру.

Так как A является максимальным левым идеалом в $\widetilde{A}$, то $\mathfrak{R}_3 \subset A$, и следовательно, $\mathfrak{R}_3$ — двусторонний идеал в A, не меняющийся при замене алгебры A противоположной алгеброй (§ 6, n° 3, следствие 2 теоремы 1). По n° 2 и определению радикала кольца с единицей, имеем $\mathfrak{R}_3 = \mathfrak{R}_1$; наконец, предложение 4 n° 1 показывает, что $\mathfrak{R}_3 = \mathfrak{R}_2$.

Определение 2. *Двусторонний идеал, определенный в предложении* 5, *называется радикалом алгебры A.*

Этот идеал также будет обозначаться $\mathfrak{R}(A)$.

Замечания. 1) Если алгебра A имеет единицу, то радикал алгебры A совпадает с радикалом кольца A, определенным в § 6, n° 3, поскольку в этом случае всякий левый идеал алгебры A регулярен.

2) Пусть $x, y \in A$. Элемент x называется *левым квазиобратным* для элемента y, или, что то же, элемент y называется *правым квазиобратным* для x, если в кольце $\widetilde{A}$ элемент $x - e$ является левым обратным для элемента $y - e$, другими словами, если $x + y - xy = 0$. Пусть $\mathfrak{R}_4$ — множество таких $x \in A$, что элемент $yx + \lambda x$ имеет левый квазиобратный при любых $y \in A$, $\lambda \in K$. Так как $yx + \lambda x - e = (y + \lambda e)\, x - e$, то $\mathfrak{R}_4$ есть множество таких $x \in A$, что элемент $zx - e$ обратим в $\widetilde{A}$ при любом $z \in \widetilde{A}$. Следовательно, $\mathfrak{R}_4$ — радикал алгебры A (§ 6, n° 3, теорема 1).

Упражнения. 1) Пусть A — алгебра над полем K такая, что $A^2 \neq A$*). Показать, что никакой идеал, содержащий A^2 и отличный от A, не регулярен.

2) Для того чтобы двусторонний идеал $\mathfrak{a}$ алгебры A был регулярным справа и слева, необходимо и достаточно, чтобы кольцо $A/\mathfrak{a}$ имело единицу.

3) Пусть $\mathfrak{a}$, $\mathfrak{b}$ — регулярные левые идеалы алгебры A.

а) Для того чтобы идеал $\mathfrak{a} \cap \mathfrak{b}$ был регулярным, необходимо и достаточно, чтобы существовали правая единица u по модулю $\mathfrak{a}$ и правая единица v по модулю $\mathfrak{b}$ такие, что $u - v \in \mathfrak{a} + \mathfrak{b}$.

*) Определения и результаты из § 6, n° 1, без изменения применяются к кольцам без единицы.

б) Вывести из а), что идеал $\mathfrak{a} \cap \mathfrak{b}$ регулярен, если один из идеалов $\mathfrak{a}$, $\mathfrak{b}$ двусторонний и регулярный справа (упражнение 2) или один из них максимален.

в) Пусть E — векторное пространство размерности 2 над полем K, A — подалгебра тензорной алгебры $T(E)$ (гл. III, § 4, n° 6), состоящая из тензоров порядка $\geqslant 1$. Показать, что левые идеалы $\mathfrak{a} = A(1 - e_1)$ и $\mathfrak{b} = A(1 - e_2)$, где (e_1, e_2) — базис пространства E над K, регулярны, но $\mathfrak{a} \cap \mathfrak{b} = \{0\}$.

4) Пусть $\mathfrak{a}$ — регулярный левый идеал алгебры A, u, v — правые единицы по модулю $\mathfrak{a}$.

а) Привести пример, в котором $u - v \overline{\in} \mathfrak{a}$ (взять $\mathfrak{a} = \{0\}$; см. § 12, упражнение 1). Получить из него пример, в котором отображение $\widetilde{\mathfrak{a}} \to \widetilde{\mathfrak{a}} \cap A$ из предложения 1 не инъективно.

б) Пусть $\mathfrak{a}$ — двусторонний идеал и алгебра $B = A/\mathfrak{a}$ не имеет таких идеалов $\mathfrak{b} \neq \{0\}$, что $B\mathfrak{b} = \{0\}$; показать, что $u - v \in \mathfrak{a}$. Так будет, в частности, если алгебра A коммутативна (см. упражнение 2).

*5) а) Пусть A — алгебра над K, E — простой модуль над алгеброй A. Показать, что либо E имеет над K размерность 1 и $AE = \{0\}$, либо для любого $x \in E$, не равного 0, имеем $Ax = E$.

б) Обратно, пусть E — модуль над кольцом A и $Ax = E$ для всякого элемента $x \in E$, отличного от 0. Показать, что на E существует единственная структура векторного пространства над полем K, которая вместе с данной структурой модуля над кольцом A определяет на E структуру модуля над алгеброй A.

в) Модуль E над алгеброй A называется *полупростым*, если он является прямой суммой простых подмодулей. Показать, что теорема плотности (§ 4, n° 2, теорема 1) остается в силе для полупростых модулей E над алгеброй A таких, что $AE = E$ (использовать а)).

6) Пусть A — алгебра над K, $\mathfrak{a}$ — ее левый идеал. Показать, что если рассматривать $\mathfrak{a}$ как алгебру над полем K, то $\mathfrak{R}(A) \cap \mathfrak{a} \subset \mathfrak{R}(\mathfrak{a})$, и если идеал $\mathfrak{a}$ двусторонний, то $\mathfrak{R}(\mathfrak{a}) = \mathfrak{R}(A) \cap \mathfrak{a}$ (доказать, что всякий простой модуль над алгеброй A является простым над алгеброй $\mathfrak{a}$ или аннулируется идеалом $\mathfrak{a}$). Привести пример не двустороннего идеала $\mathfrak{a}$ такого, что $\mathfrak{R}(\mathfrak{a}) \neq \mathfrak{R}(A) \cap \mathfrak{a}$.

*7) Пусть A — такая алгебра над K, что всякий модуль M над алгеброй A разлагается в прямую сумму подмодуля AM и подмодуля M_0, состоящего из элементов $x \in M$, аннулируемых алгеброй A. Показать, что алгебра A имеет единицу. (Взять сначала $M = \widetilde{A}_s$ (рассматриваемый как A-модуль) и установить, что A имеет правую единицу e; затем взять $M = A_s$ и установить, что $Ax \neq \{0\}$ для любого $x \in A$, отличного от 0; в заключение показать, что e является также левой единицей.)

8) Алгебра A над полем K называется *примитивной слева* (или просто *примитивной*), если существует точный простой модуль над алгеброй A. Показать, что если алгебра $\widetilde{A}$ примитивна, то алгебра A

также примитивна; обратное утверждение верно тогда и только тогда, когда алгебра A не имеет единицы. (Показать, что если точный A-модуль E не является точным $\widetilde{A}$-модулем, то в A существует правая единица e; заметить, что если e не является единицей алгебры A, то A имеет ненулевой радикал.)

9) Алгебра A над полем K называется *артиновой* (соответственно *нетеровой*), если модуль A_s над алгеброй A артинов (соответственно нетеров), то есть удовлетворяет условиям определения 1 § 2, n° 1, для подмодулей над алгеброй A. Для того чтобы алгебра A была артиновой (соответственно нетеровой), необходимо и достаточно, чтобы алгебра $\widetilde{A}$ была артиновой (соответственно нетеровой). Показать, что артинова алгебра A без радикала имеет единицу (заметить, что в этом случае алгебра $\widetilde{A}$ артинова и без радикала).

10) Показать, что если в примитивной алгебре A (упражнение 8) имеется левый идеал, конечномерный над полем K, то алгебра A конечномерна над K (и, следовательно, проста) (см. § 5, упражнение 10).

11) Показать, что нильпотентная артинова алгебра A конечномерна (применить индукцию по числу m — наименьшему из чисел k таких, что $A^k = \{0\}$).

*12) Пусть A — такая алгебра над полем K, что всякий ее левый идеал $\neq A$ имеет конечную размерность над K. Показать, что алгебра A либо конечномерна, либо является телом. (Оставив в стороне случай конечномерной алгебры A, доказать последовательно, что: 1° для любого левого идеала $\mathfrak{a} \neq A$ имеем $A\mathfrak{a} = \{0\}$ (рассмотреть эндоморфизмы $x \to ax$ векторного пространства $\mathfrak{a}$); 2° сумма $\mathfrak{b}$ всех левых идеалов алгебры A, отличных от A, отлична от A и является двусторонним идеалом, причем $A/\mathfrak{b}$ — тело (гл. I, § 9, упражнение 3); 3° если e — единица по модулю $\mathfrak{b}$, то $\mathfrak{b}e = \mathfrak{b}$ (заметить, что $Ae = A$); 4° $\mathfrak{b}A = \{0\}$ (рассмотреть правый аннулятор идеала $\mathfrak{b}$ в A, рассуждать, как в 1°), и в заключение показать, что $\mathfrak{b} = \{0\}$).

*13) Пусть A — алгебра над полем K такая, что всякая убывающая последовательность ее подалгебр стационарна. Показать последовательно, что:

а) Алгебра A артинова, и ее (нильпотентный) радикал имеет над K конечную размерность (упражнение 11).

б) Пусть B_i $(1 \leqslant i \leqslant m)$ — простые компоненты алгебры $A/\mathfrak{R}(A)$ и каждая компонента B_i изоморфна алгебре $\boldsymbol{M}_{r_i}(D_i)$, где D_i — тело с центром Z_i. Каждое тело D_i имеет конечный ранг над Z_i. (В противном случае тело D_i содержит либо трансцендентные элементы над Z_i, либо содержит бесконечную строго возрастающую последовательность подполей конечной степени над Z_i; в первом случае в D_i найдется бесконечная строго убывающая последовательность подтел, во втором случае рассмотреть коммутанты указанных подполей в D_i.)

в) Если поле Z_i имеет бесконечный ранг над K, то $r_i = 1$ (в противном случае рассмотреть нильпотентные подалгебры в B_i).

г) Поле Z_i алгебраично над K; пусть p — характеристическая экспонента поля K, L_i — наибольшее сепарабельное расширение поля K, содержащееся в Z_i; $L_i \cap Z_i^p$ имеет конечную степень над L_i^p (см. гл. V, § 8, упражнение 1).

д) Всякая убывающая последовательность подполей поля L_i, содержащих K, стационарна. В случае конечного поля K привести примеры, в которых это условие выполнено и поле L_i имеет бесконечный ранг над K, и примеры, в которых это условие не выполняется (см. гл. V, приложение II, упражнение 5).

е) Обратно, если все предыдущие условия выполнены, то всякая убывающая последовательность подалгебр алгебры A стационарна. (Используя предложение 2 § 2, n° 1, свести доказательство к случаю, когда A — тело с центром Z; пусть (D_n) — убывающая последовательность его подтел; можно считать, что тело D, порожденное подтелом D_n с центром Z_n, не зависит от n; заметить, что $D = E \otimes_S Z$, где S — подполе поля Z конечной степени над K, и E — тело, центр которого содержит S, имеющее конечный ранг над S; показать, что тогда тело D_n порождается телом E и пересечением $D_n \cap S$. Тогда доказательство сводится к случаю, где $A = Z$ — поле, радикальное расширение поля K; для любого подполя F поля Z, содержащего K, обозначим через $K(F^{p^\infty})$ пересечение подполей $K(F^{p^n})$; взяв некоторую убывающую последовательность (F_n) подполей Z, рассмотреть последовательность подполей $K(F_n^{p^\infty})$.)

*14) а) Пусть A — артинова алгебра над полем K, в которой всякая возрастающая последовательность подалгебр стационарна. Показать, что A имеет конечный ранг над полем K. (Рассуждать, как в упражнении 13; заметить, что в чистом трансцендентном расширении $K(X)$ имеется бесконечная строго возрастающая последовательность подалгебр; использовать для этого предложение 6 гл. VII, § 1, n° 5.)

б) Показать, что в алгебре многочленов $K[X]$ всякая возрастающая последовательность подалгебр стационарна. (Заметить, что подалгебра A, порожденная в $K[X]$ единицей и многочленом $f \in K[X]$ степени > 0, является кольцом главных идеалов и $K[X]$ — A-модуль конечного типа; использовать упражнение 5 гл. VII, § 2.)

ИСТОРИЧЕСКИЙ ОЧЕРК

К ГЛАВЕ VIII

(Римские цифры относятся к библиографии, находящейся в конце этого очерка.)

Мы уже видели (Исторические очерки к гл. I и гл. II и III), что первые некоммутативные алгебры появились в 1843—1844 гг. в работах Гамильтона (I) и Грассмана (III). При введении кватернионов Гамильтон уже имел вполне ясное понятие и о произвольных алгебрах конечного ранга над полем действительных чисел ((I), предисловие, стр 26—31) *). Несколько позже, развивая свою теорию, он пришел к мысли рассматривать, как он их назвал, «бикватернионы», то есть алгебру над полем комплексных чисел с той же таблицей умножения, что тело кватернионов; в связи с этим он заметил, что это расширение приводит к появлению делителей нуля (I), стр. 650). Подход Грассмана был несколько иным, и его «внешняя алгебра» долгое время оставалась в стороне от общей теории алгебр **); однако в его изложении, которому еще не хватает точности, нельзя не распознать первую идею алгебры (конечной размерности или нет) над полем действительных чисел, определенной системой образующих и соотношений (IIIb).

Новые примеры алгебр были введены более или менее явным образом в 1850—1860 гг.: если Кэли, развивая свою теорию матриц (IIc), еще не рассматривает квадратные матрицы как составляющие некоторую алгебру

---

*) Понятие изоморфизма двух алгебр у Гамильтона не встречается, но уже с этого времени математики английской школы, и особенно де Морган и Кэли, хорошо понимают, что изменение базиса не меняет существенно изучаемую алгебру (см., например, работу Кэли (IIa) об алгебрах ранга 2).

**) Причина этого, быть может, заключается в том, что Грассман, помимо «внешнего» умножения, вводит для поливекторов еще и умножения, названные им «регрессивным» и «внутренним» (они заменяют ему все, что касается двойственности). Примечательно, во всяком случае, что и около 1900 г. в статье Студи—Картана в «Энциклопедии» (XIVb) внешняя алгебра не рассматривается как одна из ассоциативных алгебр, а исследуется отдельно, и не отмечено, что один из типов алгебр ранга 4 (тип VIII на стр. 180 (XIVb)) является не чем иным, как внешней алгеброй на пространстве размерности 2.

(эта точка зрения будет ясно выражена лишь двумя Пирсами к 1870 г. (VIa)), но по крайней мере он обнаруживает в связи с этим существование системы матриц порядка 2, имеющей таблицу умножения кватернионов; это замечание можно рассматривать как первый пример линейного представления алгебры *). С другой стороны, в мемуаре, где Кэли ввел абстрактное понятие конечной группы, он мимоходом дает также определение алгебры такой группы, ничего, впрочем, из этого определения не получая ((IIb), стр. 129).

До 1870 г. заметного прогресса в рассматриваемой области не было; но к этому времени начались исследования общей структуры алгебр конечной размерности (над полем действительных или комплексных чисел). Первые шаги в этом направлении сделал Б. Пирс; он ввел понятия нильпотентного элемента, идемпотентного элемента, доказал, что алгебра (с единицей или без), в которой хотя бы один элемент не нильпотентен, имеет отличный от нуля идемпотент, написал знаменитое разложение

$$x = exe + (xe - exe) + (ex - exe) + (x - xe + exe)$$

(e — идемпотент, x — произвольный элемент) и пришел к идее (еще несколько неопределенной) о разложении идемпотента в сумму попарно ортогональных «примитивных» идемпотентов (V). Кроме того, согласно Клиффорду ((VIIc), стр. 274)**), именно Пирсу следует приписать понятие тензорного произведения алгебр, которое сам Клиффорд применял неявно при обобщении «бикватернионов» Гамильтона ((VIIa)) и явно — несколько лет спустя, при изучении алгебр, носящих его имя ((VIIb) и c)). Эти новые понятия использовались Пирсом для классификации алгебр маленькой размерности (над полем комплексных чисел) — задача, которой около 1880 г. занимались также другие математики англо-американской школы с Кэли и Сильвестром во главе. На этом пути быстро было обнаружено большое разнообра-

*) Собственно говоря, Кэли не доказывает существования этой системы матриц, не выписывает эти матрицы явно и, видимо, не замечает, что некоторые из них должны быть мнимыми (во всем мемуаре (IIc) он ни разу не уточнил, являются ли «количества», встречающиеся в матрицах, действительными или комплексными; тем не менее на стр. 494 он рассматривает все-таки комплексное число). Можно было бы подумать, что оставался всего лишь один шаг до отождествления «бикватернионов» Гамильтона и комплексных матриц порядка 2; в действительности же этот результат был сформулирован явно лишь в 1870 г. Пирсом ((V), стр. 132). Общая идея регулярного представления алгебр была предложена К. С. Пирсом около 1879 г. (VIa); эту идею уже в 1867 г. предчувствовал Лагерр ((IV), стр. 235).

**) Б. Пирс встретил Клиффорда в Лондоне в 1871 г.; и тот и другой неоднократно ссылаются на свои беседы, одна из которых, несомненно, происходила на заседании Лондонского математического общества, где Пирс сообщал о своих результатах (Proc. Lond. Math. Soc., (1), 3 (1870—1871), стр. 220).

зие возможных структур, и именно этот факт, без сомнения, побудил исследователей к поискам классов алгебр с более специальными свойствами.

На континенте, где развитие идей шло несколько иначе, подобные исследования начались незадолго до 1880 г. В 1878 г. Фробениус доказал, что кватернионы образуют единственный пример некоммутативного тела (конечной размерности) над полем действительных чисел ((VIIIa), стр. 59—63); двумя годами позже этот результат был независимо опубликован К. С. Пирсом (VIb). В 1861 г. Вейерштрасс, уточняя одно замечание Гаусса, охарактеризовал в своих лекциях коммутативные алгебры без нильпотентных элементов *) над $\boldsymbol{R}$ и $\boldsymbol{C}$ как прямые суммы полей (изоморфных $\boldsymbol{R}$ или $\boldsymbol{C}$), со своей стороны к 1870 г. к тем же результатам пришел Дедекинд в связи со своей концепцией «гиперкомплекса» в теории полей; доказательства их опубликованы в 1884—1885 гг. ((IX) и (Xa)). В этом же 1884 г. Пуанкаре в своей короткой и очень лаконичной заметке привлек внимание к тому, что уравнения $z_i = \varphi_i(x_1, \ldots, x_n, y_1, \ldots, y_n)$, выражающие мультипликативный закон в алгебре $(\sum_i x_i e_i)(\sum_i y_i e_i) = \sum_i z_i e_i$, можно рассматривать как определяющие (разумеется, локально) некоторую группу Ли. Это замечание, видимо, произвело большое впечатление на Ли и его последователей (Студи, Шефферс, Ф. Шур и несколько позже Молин и Э. Картан), именно в это время занимавшихся теорией «непрерывных» групп и особенно проблемами классификации (см., например, (XII), стр. 387); в течение 1885—1905 гг. математики этой школы в соответствии с идеей Пуанкаре применяли к изучению структуры алгебр методы, использовавшиеся ими при изучении групп и алгебр Ли. Эти методы основаны прежде всего на рассмотрении характеристического многочлена произвольного элемента алгебры относительно ее регулярного представления (этот многочлен уже встречается в указанных выше работах Вейерштрасса и Дедекинда) и разложении этого многочлена на неприводимые множители; в этом разложении, как несколько позже обнаружил Фробениус, отражается разложение регулярного представления на неприводимые компоненты.

В ходе исследований алгебр школой Ли постепенно выделились «внутренние» понятия этой теории. Понятие радикала появилось в частном случае (когда факторалгебра по радикалу — прямая композиция тел) у Г. Шеффера в 1891 г. (XII) и более отчетливо у Молина (XIIIa) и Картана (XIVa), которые изучали общий случай (само слово «радикал» принадлежит Фробениусу (VIII)). Студи и Шефферс (XII) четко определили понятие прямой композиции алгебр (предвиденное уже Б. Пирсом ((V), стр. 221)). Нако-

*) В действительности Вейерштрасс накладывает на рассматриваемые им алгебры более сильное условие, именно, что уравнение

$$a_0 + a_1 x + \ldots + a_n x^n = 0$$

(где a_i и неизвестное x лежат в алгебре) может иметь бесконечно много корней только в случае, если все a_i являются кратными одного и того же делителя 0.

нец, Молин (XIIIa) ввел понятие факторалгебры некоторой алгебры, эквивалентное, в сущности, понятию двустороннего идеала (впервые определенного Картаном (XIVa)) и гомоморфизма (название также принадлежит Фробениусу); в этих понятиях очень отчетлива связь с группами, и несколько позже, в 1904 г., Эдштейн и Веддерберн рассмотрели композиционные ряды двусторонних идеалов и распространили на них теорему Жордана — Гельдера. Наиболее значительные результаты этого периода принадлежат Ф. Молину (XIIIa). Руководствуясь аналогией с понятием простой группы, он определил простые алгебры (над C) и доказал, что они являются алгебрами матриц, а затем показал, что изучение структуры произвольной алгебры конечного ранга над C сводится, по существу, к случаю (уже изученному Шеффером), когда ее факторалгебра по радикалу является прямой суммой тел. Через некоторое время эти результаты были переоткрыты и доказаны более строго и ясно Э. Картаном (XIVa); в связи с этим Картан ввел понятие полупростой алгебры и ввел некоторые числовые инварианты («числа Картана», см. § 6, упражнение 22), связанные с произвольной алгеброй над полем C, подняв тем самым теорию этих алгебр на уровень, с тех пор еще не превзойденный *); наконец, он перенес результаты Молина и свои собственные на алгебры над R.

Около 1900 г. развитие идей привело в теории линейных алгебр к снятию всяких ограничений на поле скаляров; следует отметить, в частности, сильное влияние американской школы, группировавшейся вокруг Э. Г. Мура и Л. Э. Диксона и изучавшей конечные поля; самый замечательный результат этих исследований — теорема Веддерберна (XVIIa) о том, что всякое конечное тело — поле. В 1907 г. Веддерберн передоказал результаты Картана и распространил их на случай произвольного поля (XVIIb) при этом он полностью отказался от методов, применявшихся его предшественниками (они оказывались бесполезными, когда основное поле не является алгебраически замкнутым или максимальным упорядоченным), и возвратился к технике идемпотентов Б. Пирса, совершенствуя ее. Это позволяет ему высказать в окончательный формулировке теорему о структуре полупростых алгебр, изучение которых сводится к изучению некоммутативных тел. Кроме того, с его точки зрения, естественно возникает вопрос о расширении поля скаляров, и Веддерберн доказывает, что всякая полупростая алгебра остается полупростой при любом сепарабельном расширении основного поля **) и становится прямой композицией центральных матричных

*) Существенные трудности возникают при изучении радикала, для структурной классификации которого и до сих пор не найдено удовлетворительного принципа.

**) К тому времени, когда Веддерберн писал эти работы, понятие сепарабельного расширения еще не было определено; однако он неявно использует предположение, что если многочлен f, неприводимый над основным полем, имеет корень x в расширении этого поля, то $f'(x) \neq 0$ ((XVIIb), стр. 103). Лишь в 1929 г. Э. Нетер выяснила положение, связанное с несепарабельностью расширения поля скаляров (XXb).

алгебр, если это расширение взять достаточно большим ((XVIIb), стр. 102) *). Несколько позже Диксон при $n = 3$ (XVIII) и сам Веддерберн при произвольном n (XVIIb) построили первые примеры некоммутативных тел ранга n^2 над своим центром **), положив тем самым начало теории «скрещенных произведений» и «систем факторов», развитой позже Р. Брауером (XXIV) и Э. Нетер (XX). Наконец, в 1921 г. Веддерберн доказал один частный случай теоремы о коммутировании (XVIId).

Между тем в период с 1896 по 1910 г. в работах Фробениуса, Бернсайда и И. Шура была развита близкая к теории алгебр теория представлений линейных групп (которая ограничивалась вначале представлениями конечных групп). Эта теория идет от нескольких замечаний Дедекинда, который в 1880 г. (до опубликования его работ об алгебрах) при исследовании нормальных базисов расширений Галуа встретился с «групповым детерминантом» $\det(x_{st^{-1}})$, где $(x_s)_{s\in G}$ — последовательность переменных, множество индексов которых образует конечную группу (в других терминах, это есть норма общего элемента алгебры группы G относительно ее регулярного представления); Дедекинд обнаружил, что если группа G абелева, то этот многочлен разлагается на линейные множители (это обобщало одно тождество, доказанное задолго до этого для «циркулянтов», соответствующих циклическим группам G). В 1896 г. в очень интересной переписке с Фробениусом (Xb) Дедекинд привлекает его внимание к этому свойству, к его связи с теорией характеров абелевых групп, и к нескольким аналогичным результатам для некоторых некоммутативных групп, полученных им в 1866 г. Несколько месяцев спустя Фробениус, благодаря своему блестящему обобщению понятия характера (VIIIb), о котором мы здесь не имели возможности говорить, полностью решил проблему разложения «группового детерминанта» на неприводимые множители. Но следует отметить, что при дальнейшем развитии этой теории ***) Фробениус все время сознает ее родство

Отметим здесь еще один результат, связанный с вопросами сепарабельности (и относящийся теперь к гомологической алгебре),— разложение алгебры в прямую сумму (но не прямую композицию!) ее радикала и полупростой подалгебры. Этот результат (доказанный Молином в случае, когда поле скаляров есть $\boldsymbol{C}$ (см. § 6, упражнение 12), и Картаном — для алгебр над полем $\boldsymbol{R}$) в общей форме сформулирован Веддерберном, который доказал в действительности лишь то, что факторалгебра по радикалу проста ((XVIIb), стр. 105—109); при этом он использовал указанное выше предположение о неприводимых многочленах.

*) Арифметические исследования линейных представлений групп, начавшиеся в этот период, привели также к рассмотрению понятия, эквивалентного нейтрализующему полю представления (XVd).

**) Заметим, что Гильберт в «Основаниях геометрии» привел пример некоммутативного тела бесконечного ранга над своим центром (см. гл. IV, § 5, упражнение 10).

***) Часть результатов Фробениуса независимо получена Ф. Молином в 1897 г. (XIIIb).

с теорией алгебр (на котором, впрочем, не переставал настаивать в своих письмах Дедекинд); и поэтому, после того как он ввел для групп понятия неприводимого представления и вполне приводимого представления (VIIId) и доказал, что регулярное представление содержит все неприводимые представления, он предложил применить аналогичные методы к теории Молина — Картана (VIIIe). У Бернсайда (XVI) и И. Шура (XVb) «гиперкомплексный» аспект этой теории не выступает явно, но именно в их работах появляются на свет фундаментальные свойства неприводимых представлений, лемма Шура и теорема Бернсайда. Надо отметить, наконец, что именно в этой теории появляются впервые два частных случая теоремы о коммутировании: в диссертации Шура (XVa), где представления линейной группы связываются (именно при помощи коммутирования в кольце эндоморфизмов некоторого пространства тензоров) с представлениями симметрической группы, и в его работе 1905 г. (XVc), где он показывает, что матрицы, перестановочные со всеми матрицами неприводимого представления над полем C, являются скалярными кратными единичной матрицы I (этот результат вытекает также из теоремы Бернсайда).

Оставалось лишь ясно выявить общий субстрат этих теорий: это стало делом немецкой школы, группировавшейся вокруг Э. Нетер и Э. Артина, в работах которой в период 1925—1933 гг. и была создана современная алгебра. Уже в 1903 г. в мемуаре об алгебраическом интегрировании дифференциальных уравнений ((XIb), стр. 140—149) А. Пуанкаре ввел понятия левого и правого идеалов, минимального идеала некоторой алгебры; он заметил также, что в полупростой алгебре всякий левый идеал является прямой суммой своих пересечений с простыми компонентами и что в алгебре матриц порядка n минимальные идеалы имеют размерность n; однако его работа осталась незамеченной алгебраистами *). В 1907 г. Веддерберн заново определил левые и правые идеалы алгебры и доказал для них некоторые свойства (и главное — что радикал является наибольшим нильпотентным левым идеалом ((XVIIb), стр. 113, 114). Однако пришлось ждать 1927 г., чтобы эти понятия нашли существенное приложение в теории алгебр **). Применяя в общей форме различные доказательства, появлявшиеся в различных местах ***), В. Крулль в 1925 г. (XIXa) и Э. Нетер в 1926 г. (XXa)

*) Заметим также, что в этом мемуаре Пуанкаре отмечает, что множество операторов из групповой алгебры, аннулирующих некоторый вектор пространства линейного представления этой группы, является левым идеалом; он подчеркивает, что это замечание можно было бы применить к теории линейных представлений ((XIb), стр. 149), но эту идею никогда впоследствии не развивал.

**) Интересно отметить, что между 1907 и 1927 г. понятия левого и правого идеала появляются, но не при изучении алгебр, а в работе Э. Нетер и В. Шмейдлера (Moduln in nichtkommutativen Bereichen, Math. Zeitschr. 8 (1920), стр. 1—35), посвященной кольцам дифференциальных операторов.

***) Условие максимальности (в форме «условия обрыва возрастающих цепей») восходит к Дедекинду, который его явно ввел ((Xc), стр. 90) при

ввели и систематически использовали условия максимальности и минимальности; Крулль применяет их для обобщения на абелевы группы с операторами (которые он в связи с этим определил) теоремы Ремака о разложении конечной группы в прямое произведение неразложимых групп (см. § 2, теорема 1), в то время как Нетер использует их для характеризации дедекиндовых колец. В 1927 г. Э. Артин, применяя ту же идею к некоммутативным кольцам, показывает, как с помощью систематического изучения минимальных идеалов можно распространить теоремы Веддерберна на произвольные кольца, в которых левые идеалы удовлетворяют одновременно условиям максимальности и минимальности *).

С другой стороны, Крулль в 1926 г. (XIXb) обнаружил связь между понятиями абелевой группы с операторами и линейного представления групп; эта точка зрения была обобщена на алгебры и детально развита в 1929 г. в фундаментальной работе Э. Нетер (XXb); эта работа по важности рассмотренных идей и ясности изложения заслуживает того, чтобы вместе с мемуаром Штейница о полях считаться одним из краеугольных камней современной линейной алгебры **).

Наконец, в серии работ, начавшейся в 1927 г. ((XXI), (XXIV), (XXc)), Е. Нетер и Р. Брауер (в 1929—1931 гг. к ним присоединились А. Альберт и Х. Хассе) вновь предприняли изучение некоммутативных тел с того места, где остановились Веддерберн и Диксон. Хотя наиболее важные из их результатов состоят в углубленном изучении группы Брауера (особенно над полями алгебраических чисел) и выходят, следовательно, за рамки этой главы, отметим все же, что именно в этих работах были уточнены теоремы о коммутировании, а также понятие нейтрализующего поля простой алгебры

изучении идеалов в полях алгебраических чисел; одним из первых примеров рассуждений с «убывающими цепями» является, несомненно, пример из мемуара Веддерберна 1907 г. ((XVIIb), стр. 90), касающийся двусторонних идеалов.

*) В 1929 г. Э. Нетер показала, что эти теоремы остаются в силе, если предполагать выполненным лишь условие минимальности ((XXb), стр. 663); К. Гопкинс в 1939 г. доказал, что из этого единственного условия следует, что радикал нильпотентен.

**) Именно там вместе с прочим впервые появляются в общем виде понятия гомоморфизма группы с операторами, противоположного кольца, бимодуля, а также знаменитые «теоремы об изоморфизме» (которые в (XXa) уже сформулированы для коммутативных групп). Разумеется, частные случаи и следствия этих теорем встречались задолго до этого; например, вторая теорема об изоморфизме для конечных групп имеется у Гельдера (Math. Ann. 34 (1889)), для абелевых групп — у Дедекинда ((Xc), стр. 76, 77), для двусторонних идеалов — у Веддерберна ((XVIIb), стр. 82, 83); что касается первой теоремы об изоморфизме, то она явно сформулирована, например, Сегье в 1904 г. (Eléments de la théorie des groupes abstaits, Paris (Gauthier-Villars), 1904, стр. 65).

и его связь с максимальными подполями; наконец, в 1927 г. Сколем описывает автоморфизмы простых колец (XXIII); несколькими годами позже его теорема была переоткрыта Э. Нетер (XXc) и Р. Брауером (XXIV).

Таким образом, к 1934 г. элементарная теория простых и полупростых колец почти приняла свой окончательный вид (о состоянии теории в этот период см. (XXV)); с этого времени она стала развиваться в двух различных направлениях, по поводу которых мы ограничимся краткими замечаниями. С одной стороны, теория «систем факторов» Р. Брауера и Э. Нетер недавно получила новый толчок благодаря ее включению в современную гомологическую алгебру *). С другой стороны, сделано много попыток, более или менее успешных, распространить — хотя бы частично — результаты классической теории на кольца без условия минимальности **) и на кольца без единицы. Однако эти обобщения до сего времени не имеют откликов в других разделах математики; исключение составляют лишь определение радикала и теорема плотности, имеющие некоторые применения в топологической алгебре; желающих более подробно ознакомиться с этими работами мы отсылаем к книге Н. Джекобсона (XXVII).

---

*) Мы не можем изложить здесь историю этой теории и ее связей с понятием расширения группы с помощью другой группы; стоит, однако, отметить, что первые «системы факторов» появились как раз в связи с задачей расширения групп в 1904 г. в мемуаре И. Шура, где он заложил основы теории «проективных представлений» групп (XVb).

**) С 1928 г. Крулль распространил на произвольные полупростые модули общие теоремы о полупростых модулях конечной длины ((XIXc), стр. 63—66).

БИБЛИОГРАФИЯ

(I) W. R. Hamilton, Lectures on quaternions, Dublin, 1853.

(II) A. Cayley, Collected mathematical papers, Cambridge, 1889; a) On algebraical couples, т. I, стр. 128—130 (= Phil. Mag. (1845)); b) On the theory of groups, as depending on the symbolic equation $\theta^n = 1$, т. II, стр. 123—130 (= Phil. Mag. (1854)); c) A memoir on the theory of matrices, т. II, стр. 475—496 (=Phil. Trans. (1858)).

(III) H. Grassmann, Gesammelte math. und phys. Werke: a) Die Ausdehnungslehre von 1862, т. I_2, Leipzig (Teubner), 1896; b) Sur les differents genres de multiplication, т. II_1, p. 199—217, Leipzig (Teubner), 1904 (=J. de Crelle **XLIX** (1855)).

(IV) E. Laguerre, Œuvres, Paris (Gauthier-Villars), 1898, т. I: Sur le calcul des systèmes linéaires, p. 221—267 (=J. Ec. Polytech. **LXII**).

(V) B. Peirce, Linear associative algebra, Amer. J. Math. IV, 97—221 (1881).

(VI) C. S. Peirce: a) On the relative forms of the algebras, Amer. J. Math. IV, 221—225 (1881); b) On the algebras in which division is unambiguous, ibid., 225—229.

(VII) W. K. Clifford, Mathematical Papers, London (Macmillan), 1882: a) Preliminary sketch on biquaternions, стр. 181—200 (=Proc. Lond. Math. Soc. IV (1873); b) On the classification of geometric algebras, стр. 397—401; c) Applications of Grassmann's extensive algebras, стр. 266—276 (=Amer. J. Math. I (1878)).

(VIII) G. Frobenius: a) Ueber lineare Substitutionen und bilineare Formen, J. de Crelle **LXXXIV**, 1—63 (1878); b) Über Gruppencharaktere, Berliner Sitzungsber., 1896, стр. 985—1021; c) Über Primfaktoren der Gruppendeterminante, ibid., 1896, стр. 1343—1382; d) Darstellung der Gruppen durch lineare Substitutionen, ibid., 1897, стр. 994—1015; e) Theorie der hyperkomplexen Grössen, ibid., 1903, стр. 504—537 и 634—645.

(IX) K. Weierstrass, Mathematische Werke, т. II, Berlin (Mayer und Müller, 1895: Zur Theorie der aus n Haupteinheiten gebildeten complexen Grössen, стр. 311—332 (=Gött. Nachr. (1884)).

(X) R. Dedekind, Gesammelte mathematische Werke, Braunschweig (Vieweg), 1931—1932: a) Zur Theorie der aus n Haupteinheiten

gebildeten complexen Grössen, т. II, стр. 1—19 (=Gött. Nachr. (1885)); b) Aus Briefen an Frobenius, т. II, стр. 414—442; c) Über die Theorie der ganzen algebraischen Zahlen, т. III, стр. 1—222 (Supplement XI von Dirichlets Vorlesungen über Zahlentheorie, 4. Aufl., 1894).

(XI) H. Poincare, Œuvres, Paris (Gauthier-Villars), 1916—1954: a) Sur les nombres complexes, т. V, стр. 77—79 (=C. R. Acad. Sci. XCIX (1884); b) Sur l'intégration algébrique des équations linéaires et sur les périodes des intégrales abéliennes, т. III, стр. 106—166 (=J. Math. (5), IX (1903)).

(XII) G. Scheffers, Zurückführung complexer Zahlensysteme auf typische Formen, Math. Ann. XXXIX, 293—390 (1891).

(XIII) T. Molien: a) Ueber Systeme höherer complexer Zahlen, Math. Ann. XLI, 83—156 (1893); b) Über die Invarianten der linearen Substitutionsgruppen, Berliner Sitzungsber., 1897, стр. 1152—1156.

(XIV) E. Cartan, Œuvres complètes, Partie II, т. I, Paris (Gauthier-Villars), 1952: a) Les groupes bilinéaires et les systèmes de nombres complexes, стр. 7—105 (=Ann. Fac. Sc. Toulouse (1898)); b) Nombres complexes, стр. 107—246 (=Encycl. Sci. Math., éd. française 15 (1908)).

(XV) I. Schur: a) Über eine Klasse von Matrices, die sich einer gegebenen Matrix zuordnen lassen, Diss. Berlin, 1901; b) Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, J. de Crelle CXXVII, 20—50 (1904); c) Neue Begründung der Theorie der Gruppencharaktere, Berliner Sitzungsber., 1905, стр. 406—432; d) Arithmetische Untersuchungen über endliche Gruppen linearer Substitutionen, Berliner Sitzungsber., 1906, стр. 164—184.

(XVI) W. Burnside, On the condition of reducibility for any group of linear substitutions, Proc. Lond. Math. Soc. III, 430—434 (1905).

(XVII) J. Maclagan Wedderburn: a) A theorem of finite algebras, Trans. Amer. Math. Soc. VI, 349—352 (1905); b) On hypercomplex numbers, Proc. Lond. Math. Soc., (2), VI, 77—118 (1908); c) A type of primitive algebra, Trans. Amer. Math. Soc. XV, 162—166 (1914); d) On division algebras, Trans. Amer. Math. Soc. XXII, 129—135 (1921).

(XVIII) L. E. Dickson, Linear associative algebras and abelian equations, Trans. Amer. Math. Soc. XV, 31—46 (1914).

(XIX) W. Krull: a) Über verallgemeinerte endliche Abelsche Gruppen, Math. Zeitschr. XXIII, 161—196 (1925); b) Theorie und Anwendung der verallgemeinerten Abelschen Gruppen, Sitzungsber. Heidelberger Akad., 1926; c) Zur Theorie der allgemeinen Zahlringe, Math. Ann. XCIX, 51—70 (1928).

(XX) E. Noether: a) Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörper, Math. Ann. XCVI, 26—61 (1926); b) Hyperkomplexe Grössen und Darstellungstheorie, Math. Zeitschr.

XXX, 641—692 (1929); c) Nichtkommutative Algebra, Math. Zeitschr. **XXXVII**, 514—541 (1933).

(XXI) E. Noether und R. Brauer, Über minimale Zerfalungskörper irreduzibler Darstellungen, Berliner Sitzungsber., 1927, стр. 221—228.

(XXII) E. Artin, Zur Theorie der hyperkomplexen Zahlen, Abh. math. Sem. Univ. Hamburg V, 251—260 (1928).

(XXIII) T. Skolem, Zur Theorie der associativen Zahlensysteme, Skr. norske Vid. Akad., Oslo, 1927.

(XXIV) R. Brauer, Über Systeme hypercomplexer Zahlen, Math. Zeitschr. **XXX**, 79—107 (1929).

(XXV) M. Deuring, Algebren (Erg. der Math., т. 4), Berlin (Springer), 1937.

(XXVI) C. Hopkins, Rings with minimal conditions for left ideals, Ann. of Math. **XL**, 712—730 (1939).

(XXVII) N. Jacobson, Structure of rings, Amer. Math. Soc. Coll. Public. **XXXVII**, Providence, 1956.

ГЛАВА IX

ПОЛУТОРАЛИНЕЙНЫЕ И КВАДРАТИЧНЫЕ ФОРМЫ

Если не оговорено противное, все кольца, рассматриваемые в этой главе, предполагаются кольцами с единицей, обозначаемой 1, *все модули — унитарными и для всякого гомоморфизма* f *кольца* A *в кольцо* B *предполагается, что* $f(1) = 1$.

§ 1. Полуторалинейные формы

1. *Билинейные отображения*

В этом n° приняты следующие обозначения: A и B — кольца, E — левый A-модуль, F — правый B-модуль, G — (A,B)-*бимодуль*, то есть коммутативная группа, наделенная одновременно структурой левого A-модуля и структурой правого B-модуля, причем для любых $a \in A$, $b \in B$, $g \in G$ выполняется равенство $(ag)\,b = a\,(gb)$.

Определение 1. *Отображение* Φ *произведения* $E \times F$ *в* G *называется билинейным, если выполняются следующие условия:*

$$\Phi(x+x',\ y) = \Phi(x,\ y) + \Phi(x',\ y) \tag{1}$$

для любых $x \in E$, $x' \in E$, $y \in F$;

$$\Phi(x,\ y+y') = \Phi(x,\ y) + \Phi(x,\ y') \tag{2}$$

для любых $x \in E$, $y \in F$, $y' \in F$;

$$\Phi(ax,\ y) = a\Phi(x,\ y) \tag{3}$$

для любых $a \in A$, $x \in E$, $y \in F$;

$$\Phi(x,\ yb) = \Phi(x,\ y)\,b \tag{4}$$

для любых $x \in E$, $y \in F$, $b \in B$.

Тензорное произведение $E \otimes_Z F$ имеет каноническую структуру (A, B)-бимодуля, определенную равенством $a(x \otimes y)b = (ax) \otimes (yb)$ (гл. III, приложение II, n° 3). Задание билинейного отображения Φ произведения $E \times F$ в бимодуль G равносильно заданию такого отображения Ψ тензорного произведения $E \otimes_Z F$ в G, которое является гомоморфизмом (A, B)-бимодулей и удовлетворяет условию $\Psi(x \otimes y) = \Phi(x, y)$ для любых $x \in E$, $y \in F$.

Условия, наложенные на отображение Φ в определении 1, означают, что ограниченные на один из аргументов отображения $d_\Phi(y)$: $x \to \Phi(x, y)$ и $s_\Phi(x)$: $y \to \Phi(x, y)$ являются соответственно A-линейным отображением модуля E в модуль G и B-линейным отображением модуля F в модуль G. Наделим коммутативную группу $\mathscr{L}_A(E, G)$ (соответственно $\mathscr{L}_B(F, G)$) структурой правого B-модуля (соответственно левого A-модуля), положив $ub(x) = u(x) \cdot b$, $u \in \mathscr{L}_A(E, G)$, $x \in E$, $b \in B$ (соответственно $av(y) = a \cdot v(y)$ $(a \in A$, $v \in \mathscr{L}_B(F, G)$, $y \in F)$). Тогда условия (1)—(4) будут равносильны следующим:

$$s_\Phi(x + x') = s_\Phi(x) + s_\Phi(x'), \tag{1'}$$

$$d_\Phi(y + y') = d_\Phi(y) + d_\Phi(y'), \tag{2'}$$

$$s_\Phi(ax) = a \cdot s_\Phi(x), \tag{3'}$$

$$d_\Phi(yb) = d_\Phi(y) \cdot b \tag{4'}$$

для любых x, $x' \in E$, y, $y' \in E$, $a \in A$, $b \in B$; другими словами, отображение d_Φ модуля F в $\mathscr{L}_A(E, G)$ *B-линейно*, отображение s_Φ модуля E в $\mathscr{L}_B(F, G)$ *A-линейно*. При этом, по определению,

$$\Phi(x, y) = d_\Phi(y)(x) = s_\Phi(x)(y) \tag{5}$$

для любых $x \in E$, $y \in F$.

Определение 2. *Пусть Φ — билинейное отображение произведения $E \times F$ в G. Отображение d_Φ модуля F в $\mathscr{L}_A(E, G)$ и отображение s_Φ модуля E в $\mathscr{L}_B(F, G)$, определенные равенством* (5), *называются линейными отображениями, ассоциированными с Φ соответственно справа и слева.*

Обратно, всякое B-линейное отображение d модуля F в $\mathscr{L}_A(E, G)$ (соответственно A-линейное отображение s модуля

E в $\mathscr{L}_B(F, G)$) единственным образом с помощью формулы

$$\Phi(x, y) = d(y)(x) \quad (\text{соответственно } \Phi(x, y) = s(y)(x))$$

определяет билинейное отображение Φ произведения $E \times F$ в G, для которого d (соответственно s) является линейным отображением, ассоциированным справа (соответственно слева).

Определение 3. *Билинейное отображение* Φ *произведения* $E \times F$ *в* G *называется вырожденным справа* (соответственно *слева*), *если существует отличный от нуля элемент* $y_0 \in F$ ($x_0 \in E$) *такой, что* $\Phi(x, y_0) = 0$ *для любого* $x \in E$ (соответственно $\Phi(x_0, y) = 0$ *для любого* $y \in F$). *Отображение* Φ *называется вырожденным, если оно вырождено справа или слева.*

Для того чтобы отображение Φ было невырожденным справа (соответственно слева), необходимо и достаточно, чтобы ассоциированное с ним справа (соответственно слева) линейное отображение было *инъективным*. Отображение Φ *не вырождено*, если *оба* ассоциированных с ним линейных отображения d_Φ и s_Φ инъективны.

Пусть $(e_i)_{i \in I}$ и $(f_k)_{k \in K}$ — два семейства элементов модулей E и F, и $(a_i)_{i \in I}$ и $(b_k)_{k \in K}$ — два семейства элементов колец A и B, причем лишь конечное число этих элементов отлично от нуля. Из равенств (1)—(4) индукцией по числу ненулевых коэффициентов получается равенство

$$\Phi\Big(\sum_i a_i e_i, \ \sum_k f_k b_k\Big) = \sum_{i,\,k} a_i \Phi(e_i, f_k)\, b_k. \tag{6}$$

Если семейства (e_i) и (f_k) являются системами образующих модулей E и F, то отображение Φ полностью определяется элементами $g_{ik} = \Phi(e_i, f_k)$.

Если (e_i) и (f_k) являются базисами модулей E и F, то произвольный набор элементов $g_{ik} \in G$ ($i \in I$, $k \in K$) с помощью формулы

$$\Phi\Big(\sum_i a_i e_i, \ \sum_k f_k b_k\Big) = \sum_{i,\,k} a_i g_{ik} b_k \tag{6'}$$

определяет билинейное отображение Φ произведения $E \times F$ в G, удовлетворяющее условию $\Phi(e_i, f_k) = g_{ik}$.

В случае, когда базисы (e_i) и (f_k) конечны, матрицы $(\Phi(e_i, e_k))$ называется *матрицей отображения* Φ *относительно этих базисов.*

Билинейные отображения произведения $E \times F$ в G образуют, очевидно, *подгруппу* аддитивной группы всех отображений $E \times F$ в G. С другой стороны, если элементы $a \in A$ и $b \in B$ принадлежат *центрам* этих колец, то отображение $a\Phi b$ произведения $E \times F$ в G, определенное формулой $a\Phi b\,(x, y) = a\Phi\,(x, y)\,b$, билинейно, так что множество билинейных отображений произведения $E \times F$ в G наделяется структурой *бимодуля* над центрами колец A и B.

Пусть E' (соответственно F')— левый A-модуль (соответственно правый B-модуль), u (соответственно v)— гомоморфизм E в E' (соответственно F в F') и Φ' — билинейное отображение произведения $E' \times F'$ в G'. *Обратным образом* отображения Φ' относительно гомоморфизмов u и v называется билинейное отображение Φ произведения $E \times F$ в G, определенное равенством

$$\Phi(x, y) = \Phi'(u(x), v(y)) \qquad (x \in E,\ y \in F).$$

Легко проверяется, что для любых $x \in E$, $y \in F$ справедливы равенства

$$d_\Phi(y) = d_{\Phi'}(v(y)) \circ u \quad \text{и} \quad s_\Phi(x) = s_{\Phi'}(u(x)) \circ v.$$

Пусть Φ — билинейное отображение произведения $E \times F$ в G, и h — гомоморфизм (A, B)-бимодуля G в (A, B)-бимодуль G'. Тогда $h \circ \Phi$ является билинейным отображением произведения $E \times F$ в G'.

2. *Полуторалинейные отображения*

В этом n°, если не оговорено противное, приняты обозначения: A и B — кольца, E — левый A-модуль, F — *левый* B-модуль; $b \to b^J$ $(b \in B)$ — *антиавтоморфизм* кольца B, то есть некоторая биекция кольца B на себя, удовлетворяющая условиям: $(b + c)^J = b^J c^J$ и $(bc)^J = c^J b^J$ для любых элементов b и c кольца B; вместо J^{-1} будет употребляться знак J'; G — некоторый (A, B)-бимодуль (n° 1).

Определение 4. *Отображение произведения $E \times F$ в бимодуль G называется полуторалинейным справа относительно антиавтоморфизма J, если вместе с условиями* (1), (2), (3) (определение 1, n° 1) *выполняется условие*

$$\Phi(x, by) = \Phi(x, y) \cdot b^J \quad \textit{для любых} \quad x \in E,\ y \in F,\ b \in B. \qquad (7)$$

Если J — тождественное отображение (что возможно лишь в случае, когда кольцо B *коммутативно*), мы получаем понятие билинейного отображения.

Пусть в модулях E и F заданы произвольные семейства элементов $(e_i)_{i\in I}$ и $(f_k)_{k\in K}$, а в кольцах A и B — семейства элементов $(a_i)_{i\in I}$ и $(b_k)_{k\in K}$, лишь конечное число которых отлично от нуля. Тогда выполняется равенство

$$\Phi\left(\sum_i a_i e_i,\ \sum_k b_k f_k\right) = \sum_{i,\,k} a_i \Phi(e_i,\ f_k)\, b_k^J. \tag{8}$$

Как и в случае билинейного отображения, элементы $\Phi(e_i,\ f_k)$ однозначно определяют отображение Φ в случае, когда (e_i) и (f_k) являются системами образующих, и могут быть выбраны произвольно, если (e_i) и (f_k)— базисы модулей E и F; если (e_i) и (f_k)— конечные базисы, то матрицу $(\Phi(e_i,\ e_k))$ называют *матрицей отображения* Φ относительно этих базисов.

Как и для билинейных отображений, на множестве полуторалинейных справа отображений (относительно J) произведения $E \times F$ в бимодуль G определяется структура бимодуля над центрами колец A и B.

Понятие обратного образа для полуторалинейного отображения определяется той же формулой, что и для билинейного отображения. Впрочем, сейчас мы увидим, что изучение полуторалинейных отображений можно свести к изучению билинейных отображений.

Определение 5. *Пусть B — кольцо, F — левый* (соответственно *правый*) *B-модуль и J — антиавтоморфизм кольца B. Через F^J обозначается правый* (соответственно *левый*) *B-модуль, аддитивная группа которого совпадает с аддитивной группой модуля F, а внешняя композиция задается правилом $(b,\ y) \to b^{J'}y$* (соответственно $(b,\ y) \to yb^{J'}$) ($b \in B$, $y \in F$, $J' = J^{-1}$).

В обозначениях определения 5 линейное отображение модуля F^J в правый (соответственно левый) B-модуль H отождествляется с Z-линейным отображением u модуля F в модуль H, удовлетворяющим условию

$$u(by) = u(y)\, b^J \quad (\text{соответственно } u(yb) = b^J u(y))$$
$$(b \in B,\ y \in F).$$

Если рассматривать J как изоморфизм кольца B^0, противоположного B, на кольцо B и F — как правый (соответственно левый) B_0-модуль, то отображение u модуля F в модуль H будет *полулинейным* отображением F в H относительно изоморфизма J (гл. II, приложение I, n° 1).

Точно так же полуторалинейное справа (относительно J) отображение Φ произведения $E \times F$ в бимодуль G, где F — левый B-модуль, отождествляется с билинейным отображением произведения $E \times F^J$ в G. Если это билинейное отображение *вырождено справа* (соответственно *вырождено слева*, *невырождено*), то Φ называется *вырожденным справа* (соответственно *вырожденным слева*, *невырожденным*).

Замечание. Пусть A и B — кольца, J_1 — антиавтоморфизм кольца A, M — правый A-модуль, N — правый B-модуль и G — (A, B)-бимодуль. Отображение Φ произведения $M \times N$ в G называется *полуторалинейным слева относительно* J, если оно $\boldsymbol{Z}$-билинейно и удовлетворяет условию

$$\Phi(xa, yb) = a^{J_1}\Phi(x, y)\, b \qquad (x \in M,\ y \in N,\ a \in A,\ b \in B). \tag{9}$$

Такое отображение можно отождествить с билинейным отображением произведения $M^{J_1} \times N$ в G.

Перенесение на отображения, полуторалинейные слева, всех определений и свойств, рассмотренных для отображений, полуторалинейных справа, мы часто будем оставлять читателю, и когда мы будем говорить о полуторалинейных отображениях (без уточнения), речь будет идти об отображениях, полуторалинейных *справа*.

3. Ортогональность. Прямые суммы билинейных и полуторалинейных отображений

В этом n° приняты обозначения: A и B — кольца, E — левый A-модуль, F — правый (соответственно левый) B-модуль, G — (A, B)-бимодуль и Φ — билинейное (соответственно полуторалинейное относительно данного антиавтоморфизма J кольца B) отображение произведения $E \times F$ в G.

Определение 6. *Два элемента $x \in E$ и $y \in F$ называются ортогональными относительно отображения Φ, если $\Phi(x, y) = 0$. Два*

подмножества $E' \subset E$ *и* $F' \subset F$ *называются ортогональными, если любые два элемента* $x \in E'$ *и* $y \in F'$ *ортогональны. Множество элементов модуля* E (соответственно F), *ортогональных к некоторому подмодулю* N *модуля* F (соответственно *подмодулю* M *модуля* E), *является подмодулем модуля* E (соответственно *модуля* F); *он называется полным ортогональным подмодулем* (или просто *ортогональным подмодулем*) *для подмодуля* N (соответственно *подмодуля* M) *и обозначается через* N^0 (соответственно M^0).

Пусть H и H' — два подмодуля модуля E или модуля F. Тогда $H \subset (H^0)^0$ ($(H^0)^0$ в дальнейшем обозначается через H^{00}); если $H \subset H'$, то $H^0 \supset H'^0$. Отсюда следует, что $H^0 \supset (H^{00})^0$ и $H^0 \subset (H^0)^{00}$; положив

$$H^{000} = (H^{00})^0 = (H^0)^{00} = ((H^0)^0)^0,$$

получим $H^0 = H^{000}$.

Для того чтобы отображение Ф было вырожденным (n° 1, определение 3), необходимо и достаточно, чтобы по крайней мере один из подмодулей E^0 и F^0 был отличен от $\{0\}$. Очевидно, что значение $\Phi(x, y)$ не меняется, если к x (соответственно к y) прибавить любой элемент модуля F^0 (соответственно E^0), и следовательно, посредством факторизации Ф определяет билинейное (или полуторалинейное) отображение на произведении $(E/F^0) \times (F/E^0)$; это отображение, очевидно, не вырождено и называется *невырожденным билинейным* (или *полуторалинейным*) *отображением, ассоциированным с* Ф.

Пусть $(E_i)_{i \in I}$ — семейство левых A-модулей, $(F_i)_{i \in I}$ — семейство правых (соответственно левых) B-модулей, Φ_i — билинейное (соответственно полуторалинейное справа относительно J) отображение произведения $E_i \times F_i$ в G. Обозначим через E (соответственно F) прямую сумму модулей E_i (соответственно F_i). Тогда, очевидно, отображение Ф произведения $E \times F$ в G, определенное формулой

$$\Phi((x_i), (y_i)) = \sum_i \Phi_i(x_i, y_i) \qquad (x_i \in E_i,\ y_i \in F_i), \tag{10}$$

билинейное (соответственно полуторалинейное справа относительно J) (сумма имеет смысл, так как все слагаемые, кроме конечного числа, равны нулю). Это отображение называется *прямой суммой отображений* Φ_i. Ясно, что при $i \neq j$ модуль E_i ортого-

нален к F_j относительно Ф. Обратно, пусть Ф — билинейное или полуторалинейное отображение произведения $E \times F$ в G; пусть, далее, модуль E — прямая сумма подмодулей $(E_i)_{i\in I}$, а модуль F — прямая сумма подмодулей $(F_i)_{i\in I}$, причем для $i \neq j$ подмодуль E_i ортогонален к F_j; тогда Ф является прямой суммой своих сужений на произведения $E_i \times F_i$ $(i \in I)$.

Отображение Ф не вырождено тогда и только тогда, когда не вырождено каждое Φ_i; при этих условиях подмодуль, ортогональный к E_i, равен $\sum_{j\neq i} F_j$.

4. *Замена основных колец*

В этом n° приняты обозначения: A, B, A', B' — кольца, h и h' — гомоморфизмы колец A в A' и B в B' соответственно, G — (A, B)-бимодуль, G' — (A', B')-бимодуль, и u — гомоморфизм абелевой группы бимодуля G в абелеву группу бимодуля G', удовлетворяющий условию

$$u(agb) = h(a)\,u(g)\,h'(b) \qquad (a \in A,\ g \in G,\ b \in B). \tag{11}$$

Пусть E (соответственно F) — левый A-модуль (соответственно правый B-модуль). Напомним (гл. III, приложение II, n° 10), что если рассматривать A' (соответственно B') как правый A-модуль (соответственно левый B-модуль), то тензорное произведение $E' = A' \otimes_A E$ (соответственно $F' = F \otimes_B B'$) наделено структурой левого A'-модуля (соответственно правого B'-модуля), которая определяется формулой

$$a'_1(a' \otimes x) = (a'_1 a') \otimes x \qquad (a',\ a'_1 \in A',\ x \in E) \tag{12}$$

(соответственно $(y \otimes b)\ b'_1 = y \otimes (bb'_1)$ $(b',\ b'_1 \in B',\ y \in F)$).

Предложение 1. *Пусть E — левый A-модуль, F — правый B-модуль; положим $E' = A' \otimes_A E$ и $F' = F \otimes_B B'$. Для всякого билинейного отображения Ф произведения $E \times F$ в G существует единственное билинейное отображение Ф' произведения $E' \times F'$ в G' такое, что равенство*

$$\Phi'(a' \otimes x,\ y \otimes b') = a'u(\Phi(x, y))\,b' \tag{13}$$

выполняется для любых $a' \in A'$, $b' \in B'$, $x \in E$, $y \in F$.

Единственность отображения Ф следует из того, что E' и F' порождаются соответственно элементами $a' \otimes x$ и $y \otimes b'$. Для доказательства существования отображения Ф′ рассмотрим отображение

$$m\colon (a',\ x,\ y,\ b') \longrightarrow a'u(\Phi(x,\ y))\,b'$$

произведения $A' \times E \times F \times B'$ в G. Очевидно, это отображение $\boldsymbol{Z}$-полилинейно и удовлетворяет условиям

$$m(a',\ ax,\ y,\ b') = m(a'h(a),\ x,\ y,\ b')$$

и

$$m(a',\ x,\ yb,\ b') = m(a',\ x,\ y,\ h'(b)\,b')$$
$$(a \in A,\ b \in B,\ a' \in A',\ b' \in B',\ x \in E,\ y \in F).$$

Поэтому существует $\boldsymbol{Z}$-билинейное отображение Ф′ произведения $E' \times \Phi'$ в G', удовлетворяющее условию (13) (гл. III, приложение II, n° 1, предложение 2). Отсюда и из формулы (12), определяющей структуры модулей E' и F', следует, что Ф′ билинейно, что и заканчивает доказательство.

Сохраняя предположения и обозначения предложения 1, изучим *линейные отображения, ассоциированные с* Ф *и* Ф′ (n° 1, определение 2). Для этого построим прежде всего канонический гомоморфизм группы $\mathscr{L}_A(E,\ G)$ в группу $\mathscr{L}_{A'}(E',\ G')$. Для любого $v \in \mathscr{L}_A(E,\ G)$ отображение $(a',\ x) \to a'u(v(x))$ произведения $A' \times E$ в G' $\boldsymbol{Z}$-билинейно и в силу (11) отображает элементы $(a'h(a),\ x)$ и $(a',\ ax)$ $(a \in A)$ в один и тот же элемент бимодуля G'; следовательно (гл. III, приложение III, n°n° 1, 10), оно определяет A'-линейное в силу формулы (12) отображение $k(v)$ модуля $E' = A' \otimes_A E$ в G'; $k(v)(a' \otimes x) = a'u(v(x))$. Кроме того, из формулы (12) следует, что отображение $v \to k(v)$ группы $\mathscr{L}_A(E,\ G)$ в группу $\mathscr{L}_{A'}(E',\ G')$ удовлетворяет условию $k(vb) = k(v)\,h'(b)$ для любого $b \in B$. Пусть i — каноническое отображение $y \to y \otimes 1$ модуля F в F'. Тогда *диаграмма*

$$\begin{array}{ccc} F & \xrightarrow{d_\Phi} & \mathscr{L}_A(E,\ G) \\ \downarrow i & & \downarrow k \\ F' & \xrightarrow{d_{\Phi'}} & \mathscr{L}_{A'}(E',\ G') \end{array} \qquad (14)$$

коммутативна (d_Φ и $d_{\Phi'}$ означают здесь линейные отображения, ассоциированные справа с билинейными отображениями Ф и Ф′).

В самом деле, для любых элементов $x \in E$, $y \in F$, $a' \in A'$ имеем $d_{\Phi'}(i(y))(a' \otimes x) = \Phi'(a' \otimes x, y \otimes 1) = a'u(\Phi(x, y)) = a'u(d_{\Phi}(y)(x))$, то есть $d_{\Phi'}(i(y))(a' \otimes x) = k(d_{\Phi}(y))(a' \otimes x)$. Аналогичное соотношение коммутирования справедливо и для линейных отображений s_{Φ} и $s_{\Phi'}$, ассоциированных с Φ и Φ' слева.

Предложение 2. *Пусть J и I — антиавтоморфизмы колец B и B' соответственно, причем*

$$h'(b^J) = h'(b)^I \text{ для любого } b \in B. \tag{15}$$

Пусть, далее, E — левый A-модуль, F — левый B-модуль. Положим $E' = A' \otimes_A E$ и $F' = B' \otimes_B F$. Для любого полуторалинейного (относительно J) отображения Φ произведения $E \times F$ в G существует единственное полуторалинейное (относительно I) отображение Φ' произведения $E' \times F'$ в G', удовлетворяющее условию

$$\Phi'(a' \otimes x, y \otimes b') = a'u(\Phi(x, y))\, b'^I \tag{16}$$

для любых $a' \in A'$, $b' \in B'$, $x \in E$, $y \in F$.

Единственность отображения Φ' следует из того, что модули E' и F' порождаются соответственно тензорными произведениями $a' \otimes x$ и $y \otimes b'$. Чтобы убедиться в его существовании, рассмотрим отображение

$$m\colon (a, x, b', y) \to a'u(\Phi(x, y))\, b'^I$$

произведения $A' \times E \times B' \times F$ в G'. Это отображение, очевидно, $\boldsymbol{Z}$-полилинейно и, в силу формул (11) и (15), удовлетворяет соотношениям $m(a', ax, b', y) = m(a'h(a), x, b', y)$ и $m(a', x, b', by) = a'u(\Phi(x, y))\, h'(b^J)\, b'^I = m(a', x, b'h'(b), y)$ $(a \in A,\ b \in B,\ a' \in A',\ b' \in B',\ x \in E,\ y \in F)$. Поэтому существует $\boldsymbol{Z}$-билинейное отображение Φ' произведения $E' \times F'$ в G', удовлетворяющее условию (16) (гл. III, приложение II, п° 1, предложение 2). Отсюда и из формулы (12), определяющей структуры модулей E' и F', ввиду (15), следует, что отображение Φ полуторалинейно относительно I, что и заканчивает доказательство.

Наиболее важными являются следующие примеры (A', B')-бимодулей G' и отображений бимодуля G в G', удовлетворяющих условию (11):

1) G' — тензорное произведение $A' \otimes_A G \otimes_B B'$ (гл. III, приложение II, n° 9), u — отображение

$$g \longrightarrow 1 \otimes g \otimes 1 \qquad (g \in G)$$

бимодуля G в G'. Определенная таким образом пара (G', u) является *универсальной* в следующем смысле: для всякого (A', B')-бимодуля G'_1 и всякого $\mathbf{Z}$-линейного отображения u_1 бимодуля G в G'_1, удовлетворяющего соотношению, аналогичному (11), существует единственное $\mathbf{Z}$-линейное отображение f бимодуля G' в G'_1 такое, что $f(a'g'b') = a'f(g')\,b'$ $(a' \in A',\ g' \in G',\ b' \in B')$; другими словами, f является гомоморфизмом структур бимодулей G' и G'_1 и $u_1 = f \circ u$.

2) В случае, когда $A = B = G$ (структура (A, A)-бимодуля в кольце A определяется левыми и правыми гомотетиями), $A' = B'$ и $h = h'$, в качестве G' можно взять кольцо A', а в качестве u — гомоморфизм h кольца A в кольцо A'.

3) Предположим, что $A = B$, $A' = B'$, $h = h'$, кольца A и A' *коммутативны* и структура G как левого A-модуля совпадает с его структурой как правого A-модуля. В качестве G' тогда можно взять тензорное произведение $A' \otimes_A G$, а в качестве u — отображение $g \to 1 \otimes g$ бимодуля G в bG' (структура G' как правого A'-модуля при этом совпадает с его структурой как левого A'-модуля). Мы будем говорить тогда, что билинейное (соответственно полуторалинейное) отображение Φ', определенное предложением 1 (соответственно предложением 2), получается из отображения Φ *расширением основного кольца*, или *расширением скаляров*.

Все нижеследующее справедливо равным образом и для билинейных, и для полуторалинейных отображений; мы сохраняем ниже условия и обозначения предложения 1 (соответственно предложения 2). Для произвольного подмодуля M модуля E или F символом M' обозначим подмодуль модуля E' или F', порожденный каноническим образом модуля M.

Предложение 3. *В условиях и обозначениях предложения* 1 (соответственно *предложения* 2) *допустим, что, сверх того, A, B, A', B' — тела и что отображения α и β тензорных произведений $A' \otimes_A G$ и $G \otimes_B B'$ в бимодуль G', определенные равенствами* $\alpha(a' \otimes g) = \alpha' u(g)$ *и* $\beta(g \otimes b') = u(g)\,b'$ $(a' \in A',\ b' \in B',$

$g \in G$), *инъективны. Пусть* M *— подпространство* E, N *— подпространство* F. *Тогда подпространство* $(M')^0$ *пространства* F' *ортогональное к* M' *относительно* Φ, *равно* $(M^0)'$ *и точно так же* $(N')^0 = (N^0)'$.

В самом деле, включения $(M^0)' \subset (M')^0$ и $(N^0)' \subset (N')^0$ очевидны (впрочем, они справедливы и без предположений относительно колец A, B, A', B' и отображений α и β). Мы докажем включение $(M')^0 \subset (M^0)'$, предоставив читателю удостовериться в справедливости включения $(N')^0 \subset (N^0)'$, что делается совершенно аналогично. Пусть $y' \in (M')^0$. Тогда можно написать равенство

$$y' = \sum_{i=1}^{s} y_i \otimes b'_i \quad \left(\text{соответственно } y' = \sum_{i=1}^{s} b'_i \otimes y_i\right),$$

где $y_i \in F$ $(1 \leqslant i \leqslant s)$ и b'_i — элементы кольца B', линейно независимые над кольцом B относительно структуры B' как левого (соответственно правого) B-модуля. Пусть $x \in M$ и $x' = 1 \otimes x \in M'$ Тогда

$$0 = \Phi'(x', y') = \sum_i u(\Phi(x, y_i))\, b'_i = \beta\left(\sum_i \Phi(x, y_i) \otimes b'_i\right)$$

(соответственно

$$0 = \Phi'(x', y') = \sum u(\Phi(x, y_i))\, b'^{I}_i = \beta \sum_i \Phi(x, y_i) \otimes b'^{I}_i).$$

Но отображение β инъективно, и элементы b'_i (соответственно, ввиду формулы (15), b'^{I}_i) линейно независимы над кольцом B относительно структуры B' как левого B-модуля, так что $\Phi(x, y_i) = 0$ для всех $i = 1, \ldots, s$. Поскольку это соотношение справедливо для всех $x \in M$, то $y_i \in M^0$, $i = 1, \ldots, s$, откуда $y' \in (M^0)'$, что и требовалось доказать.

Следствие. *В предположениях и обозначениях предложения* 3 *отображение* Φ' *не вырождено тогда и только тогда, когда не вырождено отображение* Φ.

В самом деле, согласно предложению (3) справедливы равенства $(F')^0 = (F^0)'$ и $(E')^0 = (E^0)'$. С другой стороны, отображение Φ (соответственно Φ') не вырождено тогда и только тогда, когда $F^0 = E^0 = \{0\}$ (соответственно $(F')^0 = (E')^0 = \{0\}$).

Замечание. Пусть A, B, A', B' — тела. Тогда отображения α и β, определенные для бимодулей G' в рассмотренных выше трех примерах, инъективны. Это немедленно следует из результатов приложения II, n° 6, гл. III).

5. Некоторые тождества

В этом n° приняты обозначения: A — кольцо, J — антиавтоморфизм кольца A, E — левый A-модуль, G — (A, A)-бимодуль, Φ — полуторалинейное справа относительно J отображение произведения $E \times E$ в G. Положим $Q(x) = \Phi(x, x)$ $(x \in E)$.

Очевидно, что для любых $x, y \in E$ справедливы равенства

$$Q(x+y) = Q(x) + \Phi(x, y) + \Phi(y, x) + Q(y), \tag{17}$$

$$Q(x-y) = Q(x) - \Phi(x, y) - \Phi(y, x) + Q(y). \tag{18}$$

Вычитая, получим отсюда тождество

$$2(\Phi(x, y) + \Phi(y, x)) = Q(x+y) - Q(x-y). \tag{19}$$

Пусть $a \in A$. Заменив y в формуле (19) элементом ay, получим

$$2(\Phi(x, y)\, a^J + a\Phi(y, x)) = Q(x+ay) - Q(x-ay). \tag{20}$$

Умножая (19) на a (слева) и вычитая (20), получим

$$2(a\Phi(x, y) - \Phi(x, y)\, a^J) =$$

$$= aQ(x+y) - aQ(x-y) - Q(x+ay) + Q(x-ay). \tag{21}$$

Пусть, например, A — *квадратичное расширение* $K(i)$ коммутативного кольца K, где $i^2 = -1$ (гл. II, § 7, n° 7), J — K-автоморфизм $u + iv \to u - iv$ $(u, v \in K)$ кольца A, и структуры бимодуля G как правого A-модуля и левого A-модуля совпадают. Положив в (21) $a = i$, получим

$$4\Phi(x, y) = Q(x+y) - Q(x-y) + iQ(x+iy) - iQ(x-iy). \tag{22}$$

6. Билинейные и полуторалинейные формы. Ранг

В этом n° приняты обозначения: A — кольцо (соответственно кольцо с антиавтоморфизмом J), E — левый A-модуль, F — правый (соответственно левый) A-модуль. Кольцо A наделено структурой (A, A)-бимодуля, определенной правыми и левыми гомотетиями. В этом случае билинейное (соответственно полуторалинейное справа относительно J) отображение произведения $E \times F$ в бимодуль A называется *билинейной* (соответственно

полуторалинейной справа относительно J) формой на $E \times F$. Если $E = F$ (а значит, речь идет о полуторалинейной форме), то полуторалинейную форму на произведении $E \times F$ часто называют *полуторалинейной формой на модуле E.*

Пусть E и E' — левые A-модули, Φ и Φ' — полуторалинейные справа относительно J формы на E и E' соответственно. Формы Φ и Φ' называются *эквивалентными*, если существует такой изоморфизм u A-модуля E на A-модуль E', что выполняется условие: $\Phi'(u(x), u(y)) = \Phi(x, y)$ для любых элементов $x, y \in E$; тогда Φ является обратным образом формы Φ' относительно изоморфизмов u и u, а Φ' — обратный образ формы Φ относительно изоморфизмов u^{-1} и u^{-1} (n° 2).

Пусть Φ — билинейная форма на произведении $E \times F$ (F — правый A-модуль). Линейные отображения s_Φ и d_Φ, ассоциированные с формой Φ (n° 1 § 2), являются тогда соответственно отображениями модуля E в модуль F^*, *сопряженный* модулю F, и модуля F в модуль E^*, *сопряженный E.*

По определению, справедливы равенства

$$\Phi(x, y) = \langle x, d_\Phi(y)\rangle = \langle y, s_\Phi(x)\rangle. \tag{23}$$

Определим теперь линейные отображения, ассоциированные с полуторалинейной формой. Пусть J — антиавтоморфизм кольца A, и Φ — форма на произведении $E \times F$, полуторалинейная (справа) относительно J (F — левый A-модуль); положим $J' = J^{-1}$. Легко видеть, что отображение Φ' произведения $F \times E$ в кольцо A, определяемое формулой

$$\Phi'(y, x) = \Phi(x, y)^{J'} \qquad (x \in E,\ y \in F),$$

будет формой на $F \times E$, полуторалинейной справа относительно J'. В соответствии с n° 1 (определение 5) полуторалинейные формы Φ и Φ' отождествляются с билинейными формами на произведениях $E \times F^J$ и $F \times E^{J'}$. Отображения d_Φ и $d_{\Phi'}$, ассоциированные с этими билинейными формами, называются *отображениями, ассоциированными слева и справа с полуторалинейной формой* Φ, и обозначаются d_Φ и s_Φ. Следовательно, по определению,

$$\Phi(x, y) = \langle x, d_\Phi(y)\rangle = \langle y, s_\Phi(x)\rangle^J \qquad (x \in E,\ y \in F). \tag{24}$$

Таким образом, d_Φ (соответственно s_Φ) является линейным отображением модуля F^J в E^* (соответственно модуля $E^{J'}$ в F^*).

Если рассматривать J (соответственно J') как изоморфизм кольца A^0 (противоположного кольцу A) на кольцо A и F (соответственно E) как правый A^0-модуль, то d_Φ (соответственно s_Φ) будет полулинейным отображением относительно J (соответственно J') модуля F в E^* (соответственно модуля E в F^*).

Из формулы (24) и определения 6 в n° 3 немедленно следует, что для любого подмодуля N модуля F (соответственно для любого подмодуля M модуля E) выполняется равенство

$$N^0 = \overset{-1}{s}_\Phi(N') \qquad \text{(соответственно } M^0 = \overset{-1}{d}_\Phi(M')\text{)}, \tag{25}$$

где N' (соответственно M') — подмодуль сопряженного к F модуля F^* (соответственно сопряженного к E модуля E^*), *ортогональный* к N (соответственно к M) (гл. II, § 4, n° 2).

Предложение 4. *Пусть A — тело и Φ — билинейная* (соответственно *полуторалинейная относительно J*) *форма на произведении $E \times F$; для того чтобы факторпространство E/F^0 было конечномерным, необходимо и достаточно, чтобы было конечномерным факторпространство F/E^0; при этом их размерности совпадают.*

В самом деле, пусть Φ_1 — невырожденная форма на произведении $(E/F^0) \times (F/E^0)$, ассоциированная с формой Φ (n° 3). Предположим, что факторпространство E/F^0 имеет конечную размерность n. Отображение d_{Φ_1} пространства F/E^0 (соответственно $(F/E^0)^J$) в пространство $(E/F^0)^*$ инъективно, и поэтому пространство F/E^0 имеет конечную размерность $n' \leqslant n$. Точно так же, рассматривая отображение s_{Φ_1}, можно убедиться, что $n \leqslant n'$.

Следствие 1. *Пусть A — тело и форма Φ не вырождена. Для того чтобы подпространство M пространства E имело конечную размерность, необходимо и достаточно, чтобы подпространство M^0 пространства F имело конечную коразмерность, и тогда* $\operatorname{codim} M^0 = \dim M$ *и* $M^{00} = M$.

Так как $F^0 = \{0\}$, то первые два утверждения следуют из предложения 4, если применить его к сужению формы Φ на произведение $M \times F$. Кроме того, подпространство M^0 ортогонально к M^{00}, так что размерность M^{00} конечна и равна $\operatorname{codim} M^0 = \dim M$, однако $M^{00} \supset M$, так что $M^{00} = M$.

Следствие 2. *Пусть, в предположениях следствия* 1, M *и* N — *подпространства пространства* E; *тогда справедливо равенство* $(M + N)^0 = M^0 \cap N^0$; *если, кроме того,* M *и* N *конечномерны, то* $(M \cap N)^0 = M^0 + N^0$.

Первое утверждение тривиально. Пусть M и N конечномерны, и пусть $G = M^0 + N^0$; тогда, по следствию 1, $G^0 = M^{00} \cap N^{00} = M \cap N$; применив предложение 4 к сужению формы Ф на произведение $M \times G$ и пользуясь включениями $M^0 \subset G$ и $G^0 \subset M$, получим

$$\dim M/M \cap N = \dim G/M^0 = \operatorname{codim} M^0 - \operatorname{codim} G,$$

откуда, ввиду равенства $\operatorname{codim} M^0 = \dim M$, следует, что $\dim (M \cap N) = \operatorname{codim} G$. Но, по следствию 1, справедливо равенство $\dim (M \cap N) = \operatorname{codim} (M \cap N)^0$ и, кроме того, $G \subset G^{00} = (M \cap N)^0$, так что окончательно имеем $G = (M \cap N)^0$.

Предложение 4 позволяет дать следующее определение:

Определение 7. *Пусть* A — *тело* (соответственно *тело с антиавтоморфизмом* J), E — *левое векторное пространство над телом* A, F — *правое* (соответственно *левое*) *векторное пространство над телом* A, Ф — *билинейная* (соответственно *полуторалинейная относительно* J) *форма на произведении* $E \times F$. *Пусть, далее, пространства* E/F^0 *и* F/E^0 *конечномерны над телом* A. *Рангом формы* Ф *называют тогда совпадающую* (*конечную*) *размерность пространств* E/F^0 *и* F/E^0.

Если же факторпространства E/F^0 и F/E^0 бесконечномерны, то Ф — форма бесконечного ранга.

Предложение 5. *В предположениях и обозначениях определения* 7 *линейные отображения* s_Φ *и* d_Φ, *ассоциированные с формой* Ф, *имеют один и тот же ранг, равный рангу формы* Ф.

В самом деле, ядро отображения d_Φ модуля F в E^* равно, очевидно, E^0, так что ранг d_Φ равен размерности пространства F/E^0. Аналогично ранг отображения s_Φ равен размерности пространства E/F^0.

Предложение 6. *Сохраняя предположения и обозначения определения* 7, *предположим дополнительно, что пространства* E *и* F *конечномерны. Тогда следующие условия эквивалентны*:

а) d_Φ *инъективно*;
б) d_Φ *сюръективно*;
в) s_Φ *инъективно*;
г) s_Φ *сюръективно*,
д) Φ *не вырождена.*

Действительно, пространства E, F, E^* и F^* имеют конечную размерность, так что условия а) и б) эквивалентны, так же как и условия в) и г) (гл. III, § 3, n° 4). Отображения s_Φ и d_Φ имеют одинаковый ранг (предложение 5), так что а) и в) эквивалентны. Условие д) эквивалентно соотношению $E^0 = F^0 = \{0\}$ и, следовательно, оно эквивалентно конъюнкции условий а) и в), откуда и следует эквивалентность всех указанных условий.

Следствие. *Сохраняя предположения и обозначения определения* 7, *предположим, что, сверх того, пространство* E *конечномерно, а форма* Φ *не вырождена. Тогда* $\dim E = \dim F$ *и для всякого базиса* (e_i) *пространства* E $(1 \leqslant i \leqslant \dim E)$ *существует такой базис* (f_i) *пространства* F, *что* $\Phi(e_i, f_k) = \delta_{ik}$ $(i, k = 1, \ldots, \dim E)$.

В самом деле, форма Φ не вырождена, то есть $E^0 = F^0 = \{0\}$, откуда $\dim E = \dim F$ (предложение 4). Отсюда следует (предложение 6), что отображение d_Φ есть изоморфизм пространства F (соответственно F^J) на E^*; поэтому элементы $f_i = d_\Phi^{-1}(e_i^*)$, где (e_i)— базис пространства E и (e_i^*)— сопряженный базис, образуют некоторый базис пространства F, который по формуле (23) (соответственно (24)) удовлетворяет условию $\Phi(e_i, f_k) = \delta_{ik}$.

Совершенно очевидно, что в этом следствии можно поменять ролями пространства E и F, заменив при этом в доказательстве отображение d_Φ на s_Φ.

Замечание. Пусть A — кольцо с антиавтоморфизмом J, M и N — *правые* A-модули, Φ — форма на произведении $M \times N$, полуторалинейная *слева* относительно J (n° 2, замечание). Тогда справедливо равенство

$$\Phi(xa, ya') = a^J \Phi(x, y)\, a' \qquad (a, a' \in A,\ x \in M,\ y \in N).$$

Отображение Φ' произведения $N \times M$ в кольцо A, определенное формулой $\Phi'(y, x) = \Phi(x, y)^{J'}$ (где $J' = J^{-1}$), является фор-

мой, полуторалинейной слева относительно J, и формы Φ и Φ' отождествляются с билинейными формами соответственно на произведениях $M^J \times N$ и $N^{J'} \times M$. Отображения s_Φ и $s_{\Phi'}$, ассоциированные с этими билинейными формами, называются отображениями, ассоциированными слева и справа с полуторалинейной формой Φ, и обозначаются символами s_Φ и d_Φ.

Таким образом, по определению,

$$\Phi(x, y) = \langle y, s_\Phi(x)\rangle = \langle x, d_\Phi(y)\rangle^J \qquad (x \in M,\ y \in N) \tag{26}$$

и отображение s_Φ (соответственно d_Φ) является линейным отображением модуля M^J в N^* (соответственно модуля $N^{J'}$ в M^*). Для этих понятий легко сформулировать и доказать утверждения, аналогичные определению 7 и предложениям 4, 5, 6.

7. *Обратная форма для билинейной и полуторалинейной форм*

Пусть A — кольцо, E — левый A-модуль, F — правый A-модуль, Φ — билинейная форма на произведении $E \times F$. Предположим еще, что ассоциированные с формой Φ отображения, обозначаемые в дальнейшем s и d, биективны. Тогда их произведение — отображение $(s,\ d)$ — будет биекцией произведения $E \times F$ на $F^* \times E^*$ и с помощью перенесения структуры определяет на $F^* \times E^*$ билинейную форму $\hat{\Phi}$. Форма $\hat{\Phi}$ удовлетворяет, следовательно, условиям

$$\hat{\Phi}(y', x') = \Phi(s^{-1}(y'),\ d^{-1}(x')) = \\ = \langle s^{-1}(y'),\ x'\rangle = \langle d^{-1}(x'),\ y'\rangle \qquad (x' \in E^*,\ y' \in F^*). \tag{27}$$

Определение 8. *Пусть Φ — билинейная форма на произведении $E \times F$ и ассоциированные с ней отображения s и d биективны. Билинейная форма $\hat{\Phi}$, определенная равенством* (27), *называется тогда обратной формой для формы Φ.*

Пусть теперь $\hat{s}$ и $\hat{d}$ — линейные отображения модуля F^* в E^{**} и модуля E^* в F^{**}, ассоциированные слева и справа с формой $\hat{\Phi}$. По определению, для любых $x' \in E^*$ и $y' \in F^*$ выполняются равенства

$$\hat{\Phi}(y', x') = \langle y', \hat{d}(x')\rangle = \langle x', \hat{s}(y')\rangle.$$

Сравнивая эти равенства с формулой (27), получаем, что линейная форма $\hat{d}(x')$ на F^* совпадает с линейной формой, определенной элементом $d^{-1}(x')$ модуля F. Отсюда следует, что композиция $\hat{d} \circ d$ является каноническим отображением модуля F в его дважды сопряженный модуль F^{**} и, кроме того, *биективна*, так как отображения d и $\hat{d}$ биективны ($\hat{d}$ биективно по перенесению структуры); следовательно, канонически отождествляя модули F и F^{**}, имеем $\hat{d} = d^{-1}$. Аналогично модуль E канонически отождествляется с модулем E^{**}; каноническое отображение модуля E в E^{**} является композицией $\hat{s} \circ s$ и $\hat{s} = s^{-1}$. Отсюда следует, что форма, обратная к форме $\hat{\Phi}$, совпадает с Φ.

Рассмотрим теперь кольцо A с антиавтоморфизмом J, два левых A-модуля E и F и форму Φ на произведении $E \times F$, полуторалинейную справа относительно J и такую, что ассоциированные с ней отображения, обозначаемые ниже s и d, биективны. Первое уравнение в формуле (27) определяет отображение $\hat{\Phi}$ произведения $F^* \times E^*$ в кольцо A.

В соответствии с формулой (24) (n° 6) это отображение удовлетворяет условию

$$\hat{\Phi}(y', x') = \langle s^{-1}(y'), x' \rangle = \langle d^{-1}(x'), y' \rangle^J \qquad (x' \in E^*, y' \in F^*). \quad (28)$$

Очевидно, отображение $\hat{\Phi}$ Z-билинейно, и, сверх того, по определению отображений s и d, для любых $a, b \in A$, $x' \in E^*$ и $y' \in F^*$ справедливы равенства

$$\hat{\Phi}(y'a, x'b) = \Phi(a^J s^{-1}(y'), \qquad b^J d^{-1}(x')) = a^J \hat{\Phi}(y', x')\, b.$$

Поэтому $\hat{\Phi}$ является *формой* на $F^* \times E^*$, *полуторалинейной слева относительно* J (n° 2).

Определение 9. *Пусть* Φ — *форма на произведении* $E \times F$, *полуторалинейная справа относительно* J, *и ассоциированные с ней отображения* s *и* d *биективны. Форма* $\hat{\Phi}$ *на* $F^* \times E^*$, *полуторалинейная слева относительно* J, *называется обратной формой для формы* Φ.

Мы оставляем читателю определение и изучение обратной формы для формы, полуторалинейной слева. Эта обратная форма будет полуторалинейной справа.

Пусть $\hat{s}$ и $\hat{d}$ — отображения, ассоциированные с формой $\hat{\Phi}$; по формуле (26) (n° 6) справедливо равенство

$$\hat{\Phi}(y', x') = \langle y', \hat{d}(x')\rangle^J = \langle x', \hat{s}(y')\rangle. \tag{29}$$

Отображение $\hat{d}$ биективно: это следует из биективности отображения s и равенства $\langle s^{-1}(y'), x'\rangle = \langle y', \hat{d}(x')\rangle^J$, справедливого в силу формул (28) и (29). Поэтому композиция $\hat{d} \circ d$ биективна. Тогда равенство $\langle d^{-1}(x'), y'\rangle = \langle y', \hat{d}(x')\rangle$, справедливое в силу формул (28) и (29), показывает, что $\hat{d} \circ d$ является каноническим отображением модуля F в дважды сопряженный к нему модуль F^{**}.

Аналогично, отображение $\hat{s}$ биективно, и композиция $\hat{s} \circ s$ является каноническим отображением модуля E в E^{**}. Следовательно, отождествляя с помощью этих канонических отображений модуль E^{**} с E и модуль F^{**} с F, получим, что $\hat{s} = s^{-1}$, $\hat{d} = d^{-1}$, и форма Φ обратна к $\hat{\Phi}$.

Сохраняя предыдущие обозначения и предположения, возьмем в центре кольца A произвольный обратимый элемент a. Тогда по формуле (23) (соответственно (24)) отображения, ассоциированные с формой $a\Phi$, имеют вид ad и as (соответственно $a^{J'}s$) и, следовательно, биективны. Из формулы (27) следует также, что обратной формой для формы $a\Phi$ будет $a^{-1}\hat{\Phi}$ (соответственно $(a^J)^{-1}\hat{\Phi}$).

8. *Сопряженный гомоморфизм*

В этом n° приняты обозначения: A — кольцо (соответственно кольцо с антиавтоморфизмом J), E и E' — левые A-модули, F и F' — правые (соответственно левые) A-модули, Φ и Φ' — билинейные (соответственно полуторалинейные относительно J) формы соответственно на произведениях $E \times F$ и $E' \times F'$. Форма Φ предполагается *невырожденной*; другими словами (n° 1), линейные отображения d_Φ и s_Φ, ассоциированные с ней, инъективны.

Пусть u — гомоморфизм модуля E в E'. Рассмотрим множество F'_1 таких элементов $y' \in F'$, для которых существует $y \in F$, обладающий свойством $d_{\Phi'}(y') \circ u = d_\Phi(y)$, то есть $\Phi'(u(x), y') = \Phi(x, y)$ для любого $x \in E$. Множество F'_1 являет-

ся, очевидно, подмодулем модуля F'. Но отображение d_Φ инъективно, так что для каждого $y' \in F'_1$ существует единственный элемент $y \in F$ такой, что $\Phi'(u(x), y') = \Phi(x, y)$. Определенное таким образом отображение $y' \to y$ модуля F'_1 в F A-линейно; обозначив его через u^*, получим, что для любых $x \in E$ и $y \in F'_1$ справедливо равенство

$$\Phi'(u(x), y') = \Phi(x, u^*(y')). \tag{30}$$

Определение 10. *В предыдущих обозначениях и предположениях гомоморфизм u^* модуля F'_1 в F, удовлетворяющий равенству* (30), *называется сопряженным слева к гомоморфизму u; модуль F'_1 называется подмодулем определения гомоморфизма u^*.*

Точно так же определяется гомоморфизм v^*, сопряженный справа к гомоморфизму v модуля F в F':

$$\Phi'(x', v(y)) = \Phi(v^*(x'), y') \qquad (x' \in E'_1, y \in F), \tag{31}$$

где E'_1 — подмодуль модуля E', определенный аналогично модулю F'_1.

Замечание. Если гомоморфизм u^*, сопряженный слева к гомоморфизму $u\colon E \to E'$, всюду определен и отображения $s_{\Phi'}$ и $d_{\Phi'}$ инъективны, то из формулы (30) следует, что u является гомоморфизмом, сопряженным справа к u^*.

Из формулы (30) следует, что если гомоморфизмы u_1 и u_2 модуля E в E' имеют всюду определенные сопряженные гомоморфизмы и элемент c входит в центр кольца A, то

$$\left.\begin{aligned} &(u_1 + u_2)^* = u_1^* + u_2^*;\ 1^* = 1; \\ &(cu_1)^* = cu_1^*, && \text{если } \Phi \text{ и } \Phi' \text{ билинейны;} \\ &(cu_1)^* = c^J u_1^*, && \text{если } \Phi \text{ и } \Phi' \text{ полуторалинейны.} \end{aligned}\right\} \tag{32}$$

Кроме того, если E'' — третий левый A-модуль, F'' — третий правый (соответственно левый) A-модуль, Φ'' — билинейная (соответственно полуторалинейная относительно J) форма на произведении $E'' \times F''$ и u' — гомоморфизм модуля E' в E'', имеющий всюду определенный сопряженный (слева) гомоморфизм, то

$$(u' \circ u)^* = u^* \circ u'^*. \tag{33}$$

В частности, если u — *изоморфизм* модуля E на E' и сопряженные гомоморфизмы u^* и $(u^{-1})^*$ всюду определены, то u^* — изоморфизм модуля F' на F и $(u^*)^{-1} = (u^{-1})^*$. Аналогичными свойствами обладают гомоморфизмы, сопряженные справа.

Предложение 7. *Сохраняя предыдущие обозначения, предположим, что отображение d_Φ биективно. Тогда для всякого гомоморфизма и модуля E в E' сопряженный слева гомоморфизм всюду определен и* $u^* = (d_\Phi)^{-1} \circ {}^t u \circ d_{\Phi'}$.

В самом деле, если d_Φ биективно, то, в обозначениях начала этого пункта, $F'_1 = F'$, так что гомоморфизм u^* всюду определен. С другой стороны, равенство (30) равносильно следующему:

$$\langle u(x), d_{\Phi'}(y')\rangle = \langle x, (d_\Phi \circ u^*)(y')\rangle \qquad (x \in E,\ y' \in F');$$

но $\langle d_{\Phi'}(y'), u(x)\rangle = \langle {}^t u(d_{\Phi'}(y')), x\rangle$; поэтому для любого $y' \in F'$ справедливо равенство

$${}^t u(d_{\Phi'}(y')) = d_\Phi(u^*(y')), \qquad \text{то есть} \qquad {}^t u \circ d_{\Phi'} = d_\Phi \circ u^*,$$

откуда и следует доказываемое равенство.

Замечание. Если отображение s_Φ биективно, то для всякого гомоморфизма v модуля F в F' сопряженный справа гомоморфизм всюду определен и выполняется равенство

$$v^* = s_\Phi^{-1} \circ {}^t v \circ s_{\Phi'}. \tag{34}$$

Предложение 8. *Сохраняя предыдущие обозначения, предположим, что отображения s_Φ и d_Φ биективны. Пусть u и v — изоморфизмы соответственно модуля E в E' и модуля F в F'. Для того чтобы форма Φ была обратным образом формы Φ' относительно изоморфизмов u и v (то есть $\Phi(x, y) = \Phi'(u(x), v(y))$ для любых $x \in E$, $y \in F$), необходимо и достаточно, чтобы выполнялись равенства $u^{-1} = v^*$ и $v^{-1} = u^*$.*

В самом деле, равенство $\Phi'(u(x), v(y)) = \Phi(x, y)$ можно записать в виде $\Phi(x, u^*(v(y))) = \Phi(x, y)$. Поскольку это равенство выполняется для любых $x \in E$ и $y \in F$, а форма Φ не вырождена, то $u^* \circ v = 1$. По формуле (33) справедливо и равенство $v^* \circ u = 1$. Обратное утверждение также легко доказывается.

Следствие. *Пусть A — кольцо с антиавтоморфизмом J, E — левый A-модуль, Φ — форма на $E \times E$, полуторалинейная относительно J, имеющая биективные ассоциированные отображения, и u — автоморфизм A-модуля E. Для того чтобы форма Φ была инвариантной относительно автоморфизма u (то есть $\Phi(u(x), u(y)) = \Phi(x, y)$ для любых $x, y \in E$), необходимо и достаточно, чтобы сопряженные с u гомоморфизмы совпадали и выполнялось равенство $u^* = u^{-1}$.*

Это утверждение легко следует из предложения 8.

Замечание. В предположениях следствия из предложения 8 пусть, кроме того, кольцо A является телом и пространство E конечномерно над телом A. Пусть, далее, w — эндоморфизм пространства E и w_1 и w_2 — его сопряженные справа и слева гомоморфизмы. Тогда из любого из условий $ww_1 = 1$, $ww_2 = 1$, $w_1w = 1$, $w_2w = 1$ следует, что w — автоморфизм пространства E, форма Φ инвариантна относительно w, и $w_1 = w_2$.

9. *Тензорные произведения и внешние степени полуторалинейных форм*

В этом n° кольцо A предполагается *коммутативным*. Тогда всякая билинейная форма на произведении двух A-модулей является частным случаем полуторалинейной формы. Через J далее обозначается некоторый автоморфизм кольца A, J' — обратный автоморфизм.

Пусть E_i $(i = 1, \ldots, m)$ — A-модули. Отображение произведения $\prod_{i=1}^{m} E_i^J$ в $(\bigotimes_{i=1}^{m} E)^J$ (см. определение 5 n° 2), определяемое формулой

$$(x_1, \ldots, x_m) \longrightarrow x_1 \otimes \ldots \otimes x_m, \qquad x_i \in E_i^J,$$

очевидно, A-полилинейно; следовательно (гл. III, n° 7), оно определяет A-линейное отображение f произведения $\bigotimes_i E_i^J$ в $(\bigotimes_i E_i)^J$; это отображение переводит элемент $x_1 \otimes \ldots \otimes x_m$ (где знаки $\otimes$ обозначают тензорные произведения в $\bigotimes_i E_i^J$) в $x_1 \otimes \ldots \otimes x_m$ (где знаки $\otimes$ обозначают тензорные произведения в $(\bigotimes_i E_i)^J$).

Следовательно, f является изоморфизмом тензорного произведения $\bigotimes_i E_i^J$ на $(\bigotimes_i E_i)^J$. Мы будем отождествлять эти два модуля посредством построенного изоморфизма f.

Аналогично пусть E — A-модуль. Отображение модуля $(E^J)^m$ в $(\bigwedge^m E)^J$, определенное формулой

$$(x_1, \ldots, x_m) \to x_1 \wedge \ldots \wedge x_m,$$

очевидно, A-полилинейно и знакопеременно. Следовательно, оно определяет A-линейное отображение модуля $\bigwedge^m E^J$ в $(\bigwedge^m E)^J$, являющееся, как легко видеть, изоморфизмом. Мы будем отождествлять модули $\bigwedge^m E^J$ и $(\bigwedge^m E)^J$ посредством этого изоморфизма.

Пусть x' — элемент сопряженного к E модуля E^*. Отображение $x \to \langle x, x' \rangle^J$ $(x \in E)$ является элементом $(x')^J$ модуля $(E^J)^*$. Очевидно при этом, что отображение $x' \to x'^J$ является биекцией g модуля E^* на $(E^J)^*$, удовлетворяющей условию $g(ax') = a^J g(x')$ для любого $a \in A$. Далее, композиция биекции g и тождественного отображения модуля $(E^*)^J$ на E^* представляет собой изоморфизм модуля $(E^*)^J$ на модуль $(E^J)^*$. Мы будем отождествлять эти два модуля посредством указанного изоморфизма и обозначать их символом E_J^*.

Пусть E_i, F_i $(i = 1, \ldots, m)$ — A-модули, Φ_i $(i = 1, \ldots, m)$ — форма на произведении $E_i \times F_i$, полуторалинейная относительно J. Отображение произведения $E_1 \times \ldots \times E_m \times F_1^J \times \ldots \times F_m^J$ в кольцо A, определенное формулой

$$(x_1, \ldots, x_m, y_1, \ldots, y_m) \to \Phi_1(x_1, y_1)\, \Phi_2(x_2, y_2) \ldots \Phi(x_m, y_m)$$

$(x_i \in E_i,\ y_i \in F_i,\ i = 1, \ldots, m)$, A-полилинейно и, следовательно, определяет билинейную форму на произведении $(\bigotimes_i E_i) \times (\bigotimes_i F_i^J)$ (гл. III, § 1, n° 7). Поскольку второй множитель отождествлен с модулем $(\bigotimes_i F_i)^J$, тем самым на произведении $(\bigotimes_i E_i) \times (\bigotimes_i F_i)$ определена полуторалинейная относительно J

форма Φ. Эта форма характеризуется равенством

$$\Phi(x_1 \otimes \ldots \otimes x_m,\ y_1 \otimes \ldots \otimes y_m) = \prod_{i=1}^{m} \Phi_i(x_i, y_i) \quad (x_i \in E_i,\ y_i \in F_i). \tag{35}$$

Определение 11. *Пусть* E_i, F_i $(i = 1, \ldots, m)$ — *A-модули и* Φ_i $(i = 1, \ldots, m)$ — *форма на произведении* $E_i \times F_i$, *полуторалинейная относительно J. Тензорным произведением форм* Φ_i *называется полуторалинейная относительно J форма* Φ *на произведении* $(\otimes E_i) \times (\otimes F_i)$, *определенная равенством* (35).

В случае, когда все E_i и F_i равны некоторому модулю E, а все Φ_i представляют собой одну и ту же форму Ψ, форма Φ называется *продолжением формы* Ψ *на тензорную степень* $\overset{m}{\otimes} E$.

Сохраняя обозначения определения 11, изучим *отображения, ассоциированные с формой* Φ. Из формул (24) (n° 6) и (35) следует соотношение

$$\Phi(x_1 \otimes \ldots \otimes x_m,\ y_1 \otimes \ldots \otimes y_m) = \prod_{i=1}^{m} \langle x_i, d_{\Phi_i}(y_i)\rangle = \prod_{i=1}^{m} \langle y_i, s_{\Phi_i}(x_i)\rangle^J.$$

Поэтому

$$s_\Phi = j_s \circ (s_{\Phi_1} \otimes \ldots \otimes s_{\Phi_m}), \qquad d_\Phi = j_d \circ (d_{\Phi_1} \otimes \ldots \otimes d_{\Phi_m}), \tag{36}$$

где j_s (соответственно j_d) — каноническое отображение тензорного произведения $\underset{i}{\otimes} F_i^*$ в $(\underset{i}{\otimes} F_i)^*$ (соответственно произведения $\underset{i}{\otimes} E_i^*$ в $(\underset{i}{\otimes} E_i)^*$) (гл. III, § 1, n°n° 4 и 7).

Предложение 9. *Пусть A — поле с автоморфизмом J. E_i и F_i — конечномерные векторные пространства над полем A, и* Φ_i — *форма на произведении* $E_i \times F_i$, *полуторалинейная относительно J* $(1 \leqslant i \leqslant m)$. *Если все формы* Φ_i *не вырождены, то их тензорное произведение* Φ *также является невырожденной формой. В этом случае форма* $\hat{\Phi}$, *обратная к форме* Φ, *является тензорным произведением обратных форм* $\hat{\Phi}_i$.

В самом деле, поскольку A — тело, из предложений 6 и 7 гл. III, § 1, n° 3, следует, что тензорное произведение инъективных (соответственно сюръективных) линейных отображений инъективно

(соответственно сюрьективно). По предположению, отображения s_{Φ_i} биективны (предложение 6 n° 6), и поэтому их тензорное произведение также биективно. С другой стороны, каноническое отображение j_s тензорного произведения $\bigotimes_i F_i^*$ в $(\bigotimes_i F_i)^*$ биективно (гл. III, § 1, n° 5, предложение 11). Следовательно, по формуле (36) отображение s_Φ биективно, откуда и следует первое доказываемое утверждение (предложение 5 n° 6). Аналогично устанавливается биективность отображения d_Φ.

Во втором утверждении мы неявно отождествили модули $\bigotimes_i F_i^*$ и $(\bigotimes_i F_i)^*$, а также модули $\bigotimes_i E_i^*$ и $(\bigotimes_i E_i)^*$ посредством отображений j_s и j_d, являющихся в рассматриваемом случае изоморфизмами. Обратные формы, указанные в формулировке предложения, существуют, так как отображения s_{Φ_i}, d_{Φ_i}, s_Φ и d_Φ биективны (n° 7). Положим $x' = x'_1 \otimes \ldots \otimes x'_m$, $y' = y'_1 \otimes \ldots \otimes y'_m (x'_i \in E_i^*,\ y'_i \in F_i^*,\ i = 1, \ldots, m)$. По определению обратных форм и ввиду формулы (35) имеем

$$\hat{\Phi}(j_s(y'),\ j_d(x')) =$$

$$= \Phi(s_{\Phi_1}^{-1}(y'_1) \otimes \ldots \otimes s_{\Phi_m}^{-1}(y'_m),\ d_{\Phi_1}^{-1}(x'_1) \otimes \ldots \otimes d_{\Phi_m}^{-1}(x'_m)) =$$

$$= \prod_{i=1}^{m} \Phi_i(s_{\Phi_i}^{-1}(y'_i),\ d_{\Phi_i}^{-1}(x'_i)) = \prod_{i=1}^{m} \hat{\Phi}_i(y'_i, x_i),$$

откуда и следует второе утверждение. Предложение доказано.

Пусть E и F — модули над коммутативным кольцом A, Φ — полуторалинейная относительно J форма на произведении $E \times F$. Отображение произведения $E^m \times (F^J)^m$ в A, определенное формулой

$$(x_1, \ldots, x_m, y_1, \ldots, y_m) \longrightarrow \det(\Phi(x_i, y_k))$$

$$(x_i \in E,\ y_i \in F,\ i = 1, \ldots, m),$$

A-полилинейно и определяет, следовательно, билинейную форму Φ' на произведении $(\bigotimes^m E) \times (\bigotimes^m F^J)$, характеризующуюся равенством

$$\Phi'(x_1 \otimes \ldots \otimes x_m, y_1 \otimes \ldots \otimes y_m) = \det(\Phi(x_i, y_k)).$$

Так как левая часть обращается в нуль, если $x_i = x_k$ или $y_i = y_k$ $(i \neq k)$, то форма Φ' определяет посредством фактори-

зации билинейную форму на произведении $(\overset{m}{\bigwedge} E) \times (\overset{m}{\bigwedge} F^J)$ или, поскольку модуль $\overset{m}{\bigwedge} F^J$ отождествлен нами с $(\overset{m}{\bigwedge} F)^J$, полуторалинейную относительно J форму $\Phi_{(m)}$ на произведении $(\overset{m}{\bigwedge} E) \times (\overset{m}{\bigwedge} F)$. Эта форма характеризуется равенством

$$\Phi_{(m)}(x_1 \wedge \ldots \wedge x_m, y_1 \wedge \ldots \wedge y_m) = \det(\Phi(x_i, y_k)) \quad (x_i \in E,\ y_i \in F,\ i = 1, \ldots, m). \tag{37}$$

Определение 12. *Пусть E и F — A-модули и Φ — форма на $E \times F$, полуторалинейная относительно J. Тогда полуторалинейная относительно J форма $\Phi_{(m)}$ на произведении $(\overset{m}{\bigwedge} E) \times (\overset{m}{\bigwedge} F)$, определенная равенством* (37), *называется продолжением формы Φ на m-е внешние степени.*

Сохраняя обозначения определения 12, изучим *отображения, ассоциированные с формой $\Phi_{(m)}$*. Из формул (24) и (37) следуют соотношения

$$\Phi_{(m)}(x_1 \wedge \ldots \wedge x_m,\ y_1 \wedge \ldots \wedge y_m) = \det(\langle x_i, d_\Phi(y_k)\rangle) = \det(\langle y_i, s_\Phi(x_k)\rangle^J).$$

Поэтому

$$s_{\Phi_{(m)}} = k_s \circ (\overset{m}{\bigwedge} s_\Phi), \qquad d_{\Phi_{(m)}} = k_d \circ (\overset{m}{\bigwedge} d_\Phi), \tag{38}$$

где k_s (соответственно k_d) — каноническое отображение модуля $\overset{m}{\bigwedge} F^*$ в $(\overset{m}{\bigwedge} F)^*$ (соответственно $\overset{m}{\bigwedge} E^*$ в $(\overset{m}{\bigwedge} E)^*$) (см. гл. III, § 8, n° 2).

Предложение 10. *Пусть A — поле с автоморфизмом J, E и F — конечномерные векторные пространства над полем A, Φ — полуторалинейная относительно J форма на произведении $E \times F$. Если форма Φ не вырождена, то и ее продолжение $\Phi_{(m)}$ на m-е внешние степени не вырождено и форма, обратная к $\Phi_{(m)}$, является продолжением на m-е внешние степени формы $\hat{\Phi}$, обратной к Φ.*

В самом деле, по предположению, отображения s_Φ и d_Φ биективны (предложение 6, n° 6); следовательно, их внешние степени также биективны (гл. III, § 5, n° 7). С другой стороны, канонические отображения k_s и k_d биективны (гл. III, § 8, n° 2, теорема 1). Следовательно, ввиду формулы (38) отображения $s_{\Phi_{(m)}}$ и $d_{\Phi_{(m)}}$

биективны, откуда следует, что форма $\Phi_{(m)}$ не вырождена (предложение 6, n° 6). Во втором утверждении мы неявно отождествили модули $\bigwedge^m F^*$ и $(\bigwedge^m F)^*$, а также модули $\bigwedge^m E^*$ и $(\bigwedge^m E)^*$ посредством отображений k_s и k_d, являющихся в рассматриваемом случае изоморфизмами (там же). Указанные в формулировке обратные формы существуют, так как отображения s_Φ, d_Φ, $s_{\Phi_{(m)}}$ и $d_{\Phi_{(m)}}$ биективны (n° 7). Положим $x' = x'_1 \wedge \ldots \wedge x'_m$, $y' = y'_1 \wedge \ldots \wedge y'_m$ ($x'_i \in E^*$, $y'_i \in F^*$, $i = 1, \ldots, m$). По определению обратной формы (n° 7) и ввиду формулы (38) справедливо соотношение

$$\Phi_{(m)}(k_s(y'), k_d(y')) = \Phi_{(m)}(s_\Phi^{-1}(y'_1) \wedge \ldots \wedge s_\Phi^{-1}(y'_m)) =$$

$$= \Phi_m(d_\Phi^{-1}(x'_1) \wedge \ldots \wedge d_\Phi^{-1}(x'_m)) = \det(\Phi(s_\Phi^{-1}(y'_i), d_\Phi^{-1}(x'_k))) =$$

$$= \det(\hat{\Phi}(y'_i, x'_k)),$$

откуда и следует второе утверждение.

Замечание. Пусть E — *свободный* A-модуль и θ — канонический изоморфизм модуля $\bigwedge^m E$ на подмодуль антисимметрических тензоров m-го порядка (гл. III, § 5, n° 6, предложение 6). Пусть, далее, Φ — полуторалинейная форма над E, $\Phi_{(m)}$ — продолжение формы Φ на модуль $\bigwedge^m E$, и Θ — полуторалинейная форма на $\bigwedge^m E$, являющаяся обратным образом при отображении θ продолжения формы Φ на модуль $\bigotimes^m E$. По определению отображения θ и вследствие антисимметричности тензора из формулы (35) имеем равенство

$$\Theta(x_1 \wedge \ldots \wedge x_m, y_1 \wedge \ldots \wedge y_m) =$$

$$= \sum_{\sigma, \tau} \varepsilon_\sigma \varepsilon_\tau \Phi(x_{\sigma(1)}, y_{\tau(1)}) \ldots \Phi(x_{\sigma(m)}, y_{\tau(m)}),$$

где σ и τ пробегают симметрическую группу $\mathfrak{S}_m$. Используя формулу вычисления определителей и (37), это выражение перепишем в виде

$$\sum_{\tau \in \mathfrak{S}_m} \varepsilon_\tau \det(\Phi(x_i, y_{\tau(k)}) = m! \det(\Phi(x_i, y_k));$$

другими словами, $\Theta = m!\, \Phi_{(m)}$.

10. *Матричное исчисление*

В этом n° мы расширим матричное исчисление, введенное в гл. II, § 6, и заново сформулируем на новом языке некоторые результаты, доказанные в этом параграфе.

I. Пусть I и K — конечные множества индексов, H — непустое множество, и $M = (m_{ik})_{(i,k)\in I\times K}$ — матрица над множеством H (гл. II, § 6, n° 1, определение 1).

Транспонированной матрицей к матрице M называется матрица ${}^tM = (m'_{ki})_{(k,i)\in K\times I}$, определяемая условием $m'_{ki} = m_{ik}((i, k) \in I \times K)$. Очевидно,

$$ {}^t({}^tM) = M. \tag{39}$$

Это обобщает понятие транспонированной матрицы, введенное в гл. II, § 6, n° 6.

Предположим, что H — коммутативная группа (с композицией, записываемой аддитивно). Тогда множество матриц над группой H, имеющих множества индексов I и K, наделено структурой коммутативной группы, поскольку каждую матрицу можно считать отображением множества $I \times K$ в группу H. Композиция в этой группе записывается аддитивно.

Пусть H и H'— непустые множества, H — коммутативная группа (с аддитивной композицией) и f: $(h', h'') \to h'h''$ — отображение множества $H' \times H''$ в H. Пусть, далее, даны две матрицы

$$ M' = (m'_{ik})_{(i,k)\in I\times K}, \qquad M'' = (m''_{kl})_{(k,l)\in K\times L}, $$

соответственно над множествами H' и H'', такие, что множество K индексов столбцов матрицы M' совпадает с множеством индексов строк матрицы M''. *Произведением* матриц M' и M'' (в соответствии с отображением f) называется матрица $M'M''$ над группой H, определенная равенством

$$ M'M'' = \left(\sum_{k\in K} m'_{ik}m''_{kl}\right)_{(i,\,l)\in K\times L}. \tag{40}$$

Это определение обобщает понятие произведения, введенное в гл. II, § 6, n° 4. Если $H' = H'' = H$, и H — кольцо, то произведение $M'M''$ подразумевается, если не оговорено противное, вычисленным «в кольце H», то есть в соответствии с отображением $(x, y) \to xy$.

В случае, когда H' и H'' — коммутативные группы (с аддитивной композицией) и отображение f билинейно, справедливы равенства

$$ \left.\begin{aligned} (M' + M'_1)\,M'' &= M'M'' + M'_1M'', \\ M'\,(M'' + M''_1) &= M'M'' + M'M''_1, \end{aligned}\right\} \tag{41}$$

где M', M'_1 — матрицы над группой H', M'', M''_1 — матрицы над группой H'' (при этом предполагается, что все написанные суммы и произведения имеют смысл). Пусть M' и M'' — матрицы над множествами H' и H'' и f^0 — отображение произведения $H'' \times H'$ в H, определенное формулой $(h'', h') \to h'h''$; тогда выполняется равенство

$$^t(M'M'') = {}^tM''\,{}^tM', \tag{42}$$

где произведение в левой части (соответственно в правой части) вычислено в соответствии с отображением f (соответственно f^0).

Если $H' = H'' = H$, и H — кольцо, то (42) превращается в формулу (12) гл. II, § 6, n° 6.

Пусть A — кольцо, и J — антиавтоморфизм кольца A. Для всякой матрицы $M = (m_{ik})$ над кольцом A через M^J будем обозначать матрицу $(m^J{}_{ik})$. Пусть M_1 и M_2 — матрицы над кольцом A, для которых определено произведение M_1M_2. Так как J является изоморфизмом кольца A на противоположное кольцо A^0, то выполняется равенство $(M_1M_2)^J = M_1^JM_2^J$, где левая часть вычислена в кольце A, а правая — в кольце A^0. Вследствие (42) и (39) отсюда получается равенство

$$(M_1M_2)^J = {}^t({}^tM_2^J\,{}^tM_1^J), \tag{43}$$

в котором *обе* части вычислены в кольце A.

Пусть H_1, H_2, H_3, H_{12}, H_{23} и H — коммутативные группы (с аддитивной композицией), f_{12}: $H_1 \times H_2 \to H_{12}$, f_{23}: $H_2 \times H_3 \to H_{23}$, f_3: $H_{12} \times H_3 \to H$, f_1: $H_1 \times H_{23} \to H$ — билинейные отображения, и пусть M_1, M_2, M_3 — матрицы над H_1, H_2, H_3 соответственно. Если для любых $x_i \in H_i$ $(i = 1, 2, 3)$ выполняется равенство $f_3(f_{12}(x_1, x_2), x_3) = f_1(x_1, f_{23}(x_2, x_3))$, то произведения $(M_1M_2)M_3$ и $M_1(M_2M_3)$ (вычисленные в соответствии с отображениями f_{12}, f_3, f_{23} и f_1), если они имеют смысл, совпадают и обозначаются $M_1M_2M_3$.

Если $H_1 = H_2 = H_3 = H_{12} = H_{23} = H$, H — кольцо и отображения f_{12}, f_{13}, f_3, f_1 совпадают с отображением $(x, y) \to xy$, то предыдущее условие выражает ассоциативность этого отображения и, следовательно, выполнено. Аналогичные условия мы

будем считать выполненными и в случае произведения более чем трех сомножителей.

Пусть A и B — кольца, $M = (m_{ik})_{(i,k) \in I \times K}$ и $M' = (m'_{ik})_{(i,k) \in I \times K}$ — матрицы над (A, B)-бимодулем G (n° 1). Если для всякой матрицы $L = (a_i)_{i \in I}$, состоящей из одной строки, с элементами из кольца A, и всякой матрицы $C = (b_k)_{k \in K}$, состоящей из одного столбца, с элементами из кольца B, справедливо равенство $LMC = LM'C$ (произведения вычислены в соответствии с отображениями, определяющими структуру (A, B)-бимодуля G), то матрицы M и M' *совпадают*. В самом деле, положив $a_i = 1$, $a_s = 0$ для $s \neq i$ и $b_k = 1$, $b_t = 0$ для $t \neq k$, получим, что матрицы LMC и $LM'C$ будут скалярными и равными соответственно m_{ik} и m'_{ik}.

II. Рассмотрим кольцо A и A-модуль E (левый или правый), имеющий конечный базис $(e_i)_{i \in I}$. Для всякого $x \in E$ *матрицей элемента* x *относительно базиса* (e_i) называется матрица, состоящая из одного столбца, образованного координатами x_i $(i \in I)$ элемента x относительно базиса (e_i) (ср. гл. II, § 6, n° 4); эта матрица обозначается через $M(x)$ или $\boldsymbol{x}$. Чтобы напомнить, что i является индексом строки, при вычислениях удобно приписывать к нему индекс стобца, принимающий одно значение, и обозначать матрицу $M(x)$ символом (x_{i0}).

Рассмотрим теперь два A-модуля E и F (левых или правых) с конечными базисами $(e_i)_{i \in I}$ и $(f_k)_{k \in K}$; пусть (f_k^*) — базис модуля F^*, сопряженный с базисом (f_k). В нижеследующих четырех случаях мы определим относительно этих базисов матрицу отображения u модуля E в F:

(П) E и F — правые A-модули, отображение u A-линейно;

(Л) E и F — левые A-модули, отображение u A-линейно;

(ЛП) E — левый A-модуль, F — правый A-модуль, в A имеется антиавтоморфизм J, отображение u $\boldsymbol{Z}$-линейно и удовлетворяет соотношению $u(ax) = u(x)\, a^J$ $(a \in A, x \in E)$ (иными словами, u — A-линейное отображение модуля E^J в F (n° 2, определение 5)).

(ПЛ) E — правый A-модуль, F — левый A-модуль, в A имеется антиавтоморфизм J, отображение u $\boldsymbol{Z}$-линейно и удовлетворяет соотношению $u(xa) = a^J u(x)$ $(x \in E,\ a \in A)$ (иными словами, u — A-линейное отображение модуля E^J в F).

В каждом из этих случаев, *матрицей отображения* u называется матрица $(u_{ki})_{(k,i)\in K\times I}$, определяемая равенством

$$u_{ki} = \langle u(e_i), f_k^* \rangle. \tag{44}$$

В случае (П) это определение совпадает с определением в гл. II, § 6, n° 3. Матрица $M(u(x))$ образа элемента $x \in E$ задается следующими формулами:

$$M(u(x)) = M(u)\,M(x), \tag{45 П}$$

$${}^tM(u(x)) = {}^tM(x)\,{}^tM(u), \tag{45 Л}$$

$$M(u(x)) = M(u)\,M(x)^J, \tag{45 ЛП}$$

$${}^tM(u(x)) = {}^tM(x)^J\,{}^tM(u). \tag{45 ПЛ}$$

Проверим, например, равенство (45 ПЛ) (остальные проверяются аналогично и несколько проще).

Положим $x = \sum_i e_i x_{i0}$, $u(x) = \sum_k y_{k0} f_k$, тогда $u(x) = u\left(\sum_i e_i x_{i0}\right) = \sum_i x_{i0}^J u_{ki} f_k$, откуда $y_{k0} = \sum_i x_{i0}^J u_{ki}$.

Чтобы поставить оба индекса i рядом, рассмотрим транспонированные матрицы ${}^tM(x) = (x'_{0i})$, где $x'_{0i} = x_{i0}$, и ${}^tM(u) = (u'_{ik})$, где $u'_{ik} = u_{ki}$; тогда получим $y_{k0} = \sum_i x_{0i}^{\prime J} u'_{ik}$; правая часть этого равенства является элементом с индексом k матрицы ${}^tM(x)\,{}^tM(u)$, состоящей из одной строки, так что формула (45 ПЛ) доказана.

Замечания. 1) Если кольцо A коммутативно, то из равенства ${}^t(M'M'') = {}^tM''\,{}^tM'$ (см (42)), где обе части вычислены в кольце A, следует, что формула (45 Л) сводится к (45 П), а формула (45 ПЛ) — к (45 ЛП).

2) Пусть E, F, G — левые A-модули с конечными базисами, $u: E \to F$ и $v: F \to G$ — A-линейные отображения. Из формулы (45 Л) следует равенство

$${}^tM(v \circ u) = {}^tM(u)\,{}^tM(v). \tag{46}$$

В самом деле, для любого $x \in E$ имеем

$${}^tM(x)\,{}^tM(v \circ u) = {}^tM(v(u(x))) = {}^tM(u(x))^t M(v) = {}^tM(x)\,{}^tM(u)\,{}^tM(v),$$

откуда и следует (46).

Напомним, что в случае правых A-модулей

$$M(v \circ u) = M(v)\,M(u).$$

III. Пусть теперь A — кольцо, B — кольцо (соответственно кольцо с антиавтоморфизмом J, $J' = J^{-1}$), E — левый A-модуль

с конечным базисом $(e_i)_{i\in I}$ и F — правый (соответственно левый) B-модуль с конечным базисом $(f_k)_{k\in K}$. Через (e_i^*) и (f_k^*) обозначим сопряженные базисы модулей E^* и F^*. Если не оговорено противное, то рассматриваемые ниже матрицы предполагаются взятыми относительно этих базисов.

Пусть G — (A, B)-бимодуль (n° 1), Φ — билинейное (соответственно полуторалинейное справа относительно J) отображение произведения $E \times F$ в G и $R = (\Phi(e_i, f_k))$ — матрица отображения Φ. Тогда, используя введенные обозначения, перепишем формулу (6) n° 1 (соответственно (8) n° 2) в виде

$$\Phi(x, y) = {}^tM(x)\, RM(y)$$
$$(\text{соответственно } \Phi(x, y) = {}^tM(x)\, RM(y)^J), \qquad (47)$$

где произведения вычислены в соответствии с отображениями, определяющими структуру (A, B)-бимодуля G; в частности, если $A = B = G$ (в этом случае Φ — форма), эти произведения вычисляются в A.

Пусть E' — левый A-модуль с конечным базисом $(e'_s)_{s\in S}$, F' — правый (соответственно левый) A-модуль с конечным базисом $(f'_t)_{t\in T}$, $u\colon E \to E'$ и $v\colon F \to F'$ — A-линейные отображения и Φ' — билинейное (соответственно полуторалинейное справа относительно J) отображение произведения $E' \times F'$ в G. Обозначим через Φ *обратный образ* формы Φ' (относительно отображений u и v) и через U, V, R, R' — матрицы отображений u, v, Φ и Φ' относительно рассматриваемых базисов. Тогда справедливо равенство

$$R = {}^tUR'V \text{ (соответственно } R = {}^tUR'V^J), \qquad (48)$$

где произведения вычислены так же, как и в формуле (47). В самом деле, по определению, для любых $x \in E$ и $y \in F$ выполняется равенство $\Phi(x, y) = \Phi'(u(x), v(y))$, откуда по формуле (47)

$${}^tM(x)\, RM(y) = {}^tM(u(x))\, R'M(v(y))$$
$$(\text{соответственно } {}^tM(x)\, RM(y)^J = {}^tM(u(x))\, R'M(v(y))^J.$$

Из формул (45 Л) и (45 П) (соответственно (45 Л)) и формулы (43) следует равенство

$${}^tM(x)\, RM(y) = {}^tM(x)\, {}^tUR'VM(y)$$
$$(\text{соответственно } {}^tM(x)\, RM(y)^J = {}^tM(x){}^tUR'\, {}^t({}^tM(y)\, {}^tV)^J = {}^tM(x)\, {}^tUR'V^JM(y)^J),$$

что и доказывает наше утверждение.

IV. Предположим теперь, что кольца A и B совпадают и обозначим через Ф билинейную (соответственно полуторалинейную справа относительно J) форму на произведении $E \times F$ и через R — матрицу формы Ф. Найдем матрицы *ассоциированных с формой* Ф *отображений* s_Φ *и* d_Φ. Так как по формуле (23) n° 6 имеем равенство $\Phi(x, y) = \langle y, s(x)\rangle = \langle x, d(y)\rangle$ (соответственно по формуле (24), n° 6 равенство $\Phi(x, y) = \langle x, d(y)\rangle = \langle y, s(x)\rangle^J$), то верны и равенства $\Phi(e_i, f_k) = \langle f_k, s(e_i)\rangle = \langle e_i, d(f_k)\rangle$ (соответственно $\Phi(e_i, f_k) = \langle e_i, d(f_k)\rangle = \langle f_k, s(e_i)\rangle^J$). Но базис (e_i) сопряжен с базисом (e_i^*) и базис (f_k) сопряжен с базисом (f_k^*), так что, в силу (44), из последнего равенства получим

$$M(d) = R, \quad M(s) = {}^tR$$
$$\text{(соответственно } M(d) = R, \quad M(s) = {}^tR^{J'}\text{).} \tag{49}$$

Замечания. 1) Если A — тело, то линейные отображения s и d имеют одинаковый ранг. Убедимся, что и их матрицы $M(s)$ и $M(d)$ имеют одинаковый ранг; в самом деле, ранг всякой матрицы над телом A равен рангу ее транспонированной матрицы (гл. II, § 6, n° 7, предложение 3). В случае полуторалинейного отображения Ф из равенства рангов матриц R над телом A и ${}^tR$ над телом A^0 (там же), учитывая, что J' является изоморфизмом тела A^0 на A, можно заключить, что матрицы R и ${}^tR^J$ над телом A имеют одинаковый ранг.

2) Пусть M и N — правые A-модули с конечными базисами (m_i) и (n_k), Ф — форма на $M \times N$, полуторалинейная слева относительно J (n° 6, замечание), s и d — ассоциированные с ней отображения, $R = (\Phi(m_i, n_k))$ — матрица формы Ф. Тогда из формул (26) n° 6 следуют равенства

$$M(d) = R^{J'}, \qquad M(s) = {}^tR.$$

Предположим теперь, что отображения s и d, ассоциированные с формой Ф, биективны, и вычислим матрицу $\hat{R}$ *обратной формы* $\hat{\Phi}$ (n° 7). Если Ф — билинейная форма, то Ф является обратным образом формы $\hat{\Phi}$ относительно линейных отображений $s\colon E \to F^*$ и $d\colon F \to E^*$; значит, ввиду равенств (48) и (49), $R = R\hat{R}R$, откуда, поскольку матрица R обратима (d — биекция), следует, что $\hat{R} = R^{-1}$. Это равенство справедливо и для полуторалинейной формы Ф, так как, рассмотрев Ф как билинейную форму на произведении $E \times F^J$ и отождествив $(F^J)^*$ с $(F^*)^J$ (ср. n° 9), получим, что обратная форма для этой билинейной фор-

мы совпадает с Ф, рассматриваемой как билинейная форма на произведении $(F^*)^J \times E^*$. В обоих случаях *матрица обратной формы* $\hat{\Phi}$ *обратна к матрице формы* Ф.

Пусть, наконец, E' — левый A-модуль и F' — правый (соответственно левый) A-модуль с конечными базисами (e'_s) и (f'_t); пусть, далее, Φ' — билинейная (соответственно полуторалинейная относительно J) форма на произведении $E' \times F'$, и R' — ее матрица. Предположим, что отображения s_Φ и d_Φ биективны. Пусть $u\colon E \to E'$ и $v\colon F \to F'$ — линейные отображения, $u^*\colon F' \to F$ и $v^*\colon E' \to E$ — их сопряженные гомоморфизмы (n° 8, предложение 7); обозначим через U, V, U^*, V^* матрицы отображений u, v, u^*, v^* относительно данных базисов. Тогда справедливы равенства

$$U^* = R^{-1}\,{}^tU R', \qquad {}^tV^* = R'VR^{-1} \tag{50}$$

(соответственно $U^{*J} = R^{-1}\,{}^tU\,R'$, ${}^tV^* = R'V^JR^{-1}$).

В самом деле, для любых $x \in E$ и $y \in F'$ имеем равенство $\Phi'(u(x), y) = \Phi(x, u^*(y))$ (n° 8, определение 10). Если Ф — билинейная форма, то по формуле (47) ${}^tM(u(x))\,R'\,M(y) = {}^tM(x)\,R\,M(u^*(y))$; отсюда по (45 Л) и (45 П) следует равенство ${}^tM(x)\,{}^tU\,R'\,M(y) = {}^tM(x)\,RU^*\,M(y)$, так что ${}^tUR' = RU^*$, то есть первая формула доказана (так как отображение d биективно, а матрица R обратима). Если Ф— полуторалинейная форма, то из (47) и (45 Л) следует равенство ${}^tM(x)\,{}^tUR'M(y)^J = {}^t(M(x)\,R^t({}^tM(y)\,{}^tU^*)^J$; но в силу (43) $({}^tM(y)\,{}^tU^*)^J = {}^t({}^{tt}U^{*J}.{}^{tt}M(y)^J)$, откуда ${}^t({}^tM(y)\,{}^tU^*)^J = U^{*J}.M(y)^J$; следовательно, ${}^tM(x)\,{}^tUR'M(y)^J = {}^tM(x)\,RU^{*J}\,M(y)^J$, и поэтому ${}^tUR' = RU^{*J}$ и $U^{*J} = R^{-1}.{}^tUR'$. Доказательство формул для матрицы V^* аналогично.

Упражнения. 1) Пусть A — поле, E — векторное пространство над полем A, имеющее счетный бесконечный базис $(e_n)_{n\geqslant 1}$. Определим билинейную форму Ф на пространстве E, положив $\Phi(e_{i+1}, e_i) = 1$ для $i \geqslant 1$, $\Phi(e_k, e_j) = 0$ для $k \neq j+1$ и $j \geqslant 1$. Показать, что линейное отображение d_Φ, ассоциированное справа с формой Ф, инъективно, а линейное отображение s_Φ, ассоциированное с формой Ф слева, не инъективно.

2) Пусть E — $\boldsymbol{Z}$-модуль, являющийся прямой суммой модулей $\boldsymbol{Z}$ и $\boldsymbol{Z}/(2)$, и E^* — сопряженный модуль (изоморфный $\boldsymbol{Z}$). Показать, что для билинейной формы $(x, x') \to \langle x, x'\rangle$ на произведении

$E \times E^*$ линейное отображение, ассоциированное справа, инъективно, а линейное отображение, ассоциированное слева, не инъективно.

3) Привести пример билинейной формы Φ на произведении двух векторных пространств, для которой отображение d_Φ биективно, а отображение s_Φ инъективно, но не биективно (взять бесконечномерное пространство E и сопряженное к нему пространсто F; см. гл. II, § 5, упражнение 3).

4) Пусть A — кольцо с антиавтоморфизмом J, E — правый A-модуль, G — (A, A)-бимодуль и Φ — отображение произведения $E \times E$ в G, полуторалинейное справа относительно J. Положим $Q(x) = \Phi(x, x)$. Доказать тождество

$$2\Phi(x, y)(\mu^J\lambda^J - \lambda^J\mu^J) = Q(x - \mu\lambda y) - Q(x + \mu\lambda y) + \mu Q(x + \lambda y) - \\ - \mu Q(x - \lambda y) + Q(x + \mu y)\lambda^J - Q(x - \mu y)\lambda^J + \\ + \mu Q(x - y)\lambda^J - \mu Q(x + y)\lambda^J.$$

5) Пусть K — поле характеристики 2, A — сепарабельное квадратичное расширение поля K, $A = K(\theta)$, где θ — корень некоторого неприводимого многочлена $X^2 + X + \beta$ из кольца $K[X]$. Пусть, далее, J — K-автоморфизм поля A, отличный от тождественного и такой, что $\theta^J = \theta + 1$ (гл. V, § 11, упражнение 8); E, G — векторные пространства над полем A. Показать, что для всякого полуторалинейного (относительно J) отображения Φ произведения $E \times E$ в G справедливо тождество

$$\Phi(x, y) = Q(\theta x + y) - \beta Q(x) - Q(y) - (\theta + 1)(Q(x + y) - Q(x) - Q(y)),$$

где $Q(x) = \Phi(x, x)$.

6) Пусть A — тело, E — векторное пространство над телом A, Φ — полуторалинейная форма на пространстве E, u — эндоморфизм пространства E.

а) Для того чтобы существовал единственный эндоморфизм u^* пространства E, удовлетворяющий условию $\Phi(u(x), y) = \Phi(x, u^*(y))$ для любых $x, y \in E$, необходимо и достаточно, чтобы отображение d_Φ было инъективно и выполнялось включение

$$^t u(d_\Phi(E)) \subset d_\Phi(E).$$

б) Привести пример, в котором пространство E бесконечномерно, отображение d_Φ инъективно, но $^t u(d_\Phi(E))$ не содержится в $d_\Phi(E)$.

7) Пусть E, E_1 — A-модули, Φ (соответственно Φ_1) — полуторалинейная форма на модуле E (соответственно E_1). Предположим, что форма Φ_1 не вырождена и что существуют такой элемент $\alpha \in A$ и такая биекция u модуля E на E_1, что для любых $x, y \in E$ выполняется равенство $\Phi_1(u(x), u(y)) = \Phi(x, y)\alpha$. Показать, что: 1° форма Φ невырождена; 2° отображение u *линейно*; 3° если A-модуль E_1 точный, то модуль E также точный; 4° если форма Φ_1 принимает значения,

не являющиеся в кольце A левыми делителями нуля, то форма Φ также принимает такие значения.

8) Пусть A — тело, E_1, E_2 — векторные пространства над A, отличные от 0, Φ_1 (соответственно Φ_2) — невырожденная форма на пространстве E_1 (соответственно E_2), полуторалинейная относительно антиавтоморфизма J_1 (соответственно J_2) тела A. Пусть u — линейное отображение пространства E_1 *на* E_2 такое, что из равенства $\Phi_1(x, y) = 0$ следует $\Phi_2(u(x), u(y)) = 0$.

а) Показать, что отображение u — биекция пространства E_1 на E_2. (Показать, что при $u(0) \neq 0$ в пространстве E_1 нашлись бы такие два вектора a и b, что $u(a) \neq 0$, $u(b) = 0$ и $\Phi_1(a, b) \neq 0$; заметить, что тогда было бы справедливо равенство $u(H) = E_2$, где H — гиперплоскость, состоящая из векторов $x \in E_1$ таких, что $\Phi_1(a, x) = 0$.)

б) Показать, что если $\dim E_1 \geqslant 2$, то существует элемент $\alpha \in A$ такой, что $\Phi_2(u(x), u(y)) = \Phi_1(x, y)\alpha$ для любых x, $y \in E_1$. (Показать, что для любого $y \in E_1$ существует элемент $m(y) \in A$ такой, что $\Phi_2(u(x), u(y)) = \Phi_1(x, y)\, m(y)$ для любого $x \in E_1$, и что если y и y' линейно независимы в E_1, то $m(y + y') = m(y) = m(y')$.)

9) Пусть A — тело, E и F — левые векторные пространства над A, Φ — невырожденная форма на произведении $E \times F$, полуторалинейная относительно антиавтоморфизма J тела A.

а) Пусть M — подпространство в E, N — подпространство в F, причем $N \supset M^0$ и $M \supset N^0$. Показать, что если одно из пространств N/M^0 и M/N^0 конечномерно, то и другое конечномерно и размерности этих пространств совпадают.

б) Пусть M и M' — подпространства в E, $M^{00} = M$ и подпространство M' конечномерно; показать, что $(M \cap M')^0 = M^0 + M'^0$ и $(M + M')^{00} = M + M'$. (Применив а) к подпространствам M' и $M^0 + M'^0$, показать, что $\dim(M \cap M') = \operatorname{codim}(M^0 + M'^0)$, применив а) к подпространствам $M + M'$ и M^0, показать, что

$$\dim((M + M')^{00}/M) = \dim((M + M')/M).$$

в) Показать, что если $E = F$ и $E = M^0 + M^{00}$, где M — некоторое подпространство в E, то E является прямой суммой подпространств M^0 и M^{00}.

г) Пусть E — векторное пространство над полем A, обладающее счетным бесконечным базисом $(e_n)_{n \geqslant 0}$, и Φ — симметрическая билинейная форма на пространстве E такая, что $\Phi(e_n, e_n) = 1$ для любого n, $\Phi(e_i, e_j) = 0$ для $i \geqslant 1$, $j \geqslant 1$ и $i \neq j$ и $\Phi(e_0, e_n) = 1$ для всех $n \geqslant 1$. Показать, что форма Φ невырождена. Пусть M (соответственно N) — подпространство, порожденное в E элементами e_{2k} (соответственно e_{2k-1}) для $k \geqslant 1$, так что $H = M + N$ — гиперплоскость в пространстве E. Показать, что $M^0 = N$, $N^0 = M$, $H^{00} = E \neq H$, $(M \cap N)^0 \neq M^0 + N^0$, $(M + N)^{00} \neq M + N$, а также $M^{00} = M$ и $N^{00} = N$. Показать, что $(L \cap H)^0 \neq L^0 + H^0$, где L — подпространство размерности 2, порожденное элементами e_0 и e_1.

*10) Пусть E, E' — левые векторные пространства размерности $\geqslant 3$ над телами A, A' соответственно; пусть $\mathfrak{F}(E)$ (соответственно $\mathfrak{F}(E')$) — решеточно-упорядоченное (по включению) множество конечномерных подпространств пространства E (соответственно E').

а) Пусть отображение p множества $\mathfrak{F}(E)$ в $\mathfrak{F}(E_1)$ удовлетворяет условиям: для любого $M \in \mathfrak{F}(E)$, $\dim p(M) = \dim M$ и для любой пары элементов M, N множества $\mathfrak{F}(E)$ $p(M+N) = p(M)+p(N)$. Показать, что отображение p инъективно; если отображение p биективно, то существует полулинейное биективное отображение u пространства E в E' такое, что для любого $M \in \mathfrak{F}(E)$ выполняется равенство $u(M) = p(M)$ (использовать упражнение 10 гл. II, приложение III).

б) Привести пример, в котором $A' = A$ коммутативно, пространство $E' = E$ конечномерно и существует отображение p множества $\mathfrak{F}(E)$ в себя, при котором

$$\dim p(M) = \dim M,\ p(M+N) = p(M)+p(N),\ p(M \cap N) = p(M) \cap p(N),$$

но не существует инъективного полулинейного отображения пространства E в себя такого, что $u(M) = p(M)$ для любого $M \in \mathfrak{F}(E)$. (Рассмотреть случай, когда существует надполе A'' поля A, имеющее конечную степень и изоморфное полю A, например $A = F_p(X)$, где p — простое число; тогда векторное пространство $E'' = A'' \otimes_A E$ над полем A'' имеет ту же размерность, что пространство E над полем A; рассмотреть отображение $M \to A'' \otimes_A M$.)

в) Возьмем $A' = A$. Пусть ω — биективное отображение множества $\mathfrak{F}(E)$ на множество $\mathfrak{F}'(E')$ подпространств пространства E', имеющих конечную факторразмерность, причем $\operatorname{codim} \omega(M) = \dim M$ и $\omega(M+N) = \omega(M) \cap \omega(N)$. Показать, что на произведении $E \times E'$ существует полуторалинейная форма Φ, невырожденная справа и такая, что $\omega(M) = M^0$ для любого $M \in \mathfrak{F}(E)$ (использовать теорему 1 гл. II, § 4, п° 6).

11) а) Пусть кольцо A артиново слева и справа (гл. VIII, § 2, п° 3). Показать, что следующие условия эквивалентны: 1° правый (соответственно левый) аннулятор всякого левого (соответственно правого) идеала, отличного от A, не равен 0; 2° для любого простого левого (соответственно правого) A-модуля сопряженный модуль отличен от 0; 3° для всякого левого (соответственно правого) A-модуля конечного типа сопряженный модуль отличен от 0. Говорят, что кольцо A удовлетворяет условию (N_s) (соответственно (N_d)), если для любых левых (соответственно правых) A-модулей выполняются указанные условия.

б) Пусть кольцо A артиново слева и справа и удовлетворяет условию (N_d), E (соответственно F) — *свободный* левый (соответственно правый) A-модуль, имеющий счетный базис над кольцом A.

Ф — билинейная форма на произведении $E \times F$ и отображение s_Φ инъективно. Пусть M — свободный подмодуль в E. Показать, что существуют свободный подмодуль N модуля F и такой базис (e_n) (соответственно (f_n)) модуля E (соответственно F), что $\Phi(e_i, f_j) = \delta_{ij}$; более того, в качестве e_1 можно взять произвольный элемент подмодуля M. (Заметить, что если x — свободный элемент модуля M, то образом модуля F при отображении $y \to \Phi(x, y)$ будет все кольцо A; затем по индукции построить базисы (e_n) и (f_n).) Вывести отсюда, что если базис (e_n) подмодуля M конечен, то модуль E является прямой суммой подмодулей M и N^0, причем $M^{00} = M$.

в) Сохраняя предположения пункта б), предположим дополнительно, что кольцо A удовлетворяет условию (N_s) и что отображение d_Φ инъективно. Показать, что в этом случае в пространствах E и F существуют базисы (e_n) и (f_n) такие, что $\Phi(e_i, f_j) = \delta_{ij}$ (используя б), строить по индукции попеременно элементы базисов (e_n) и (f_n)).

°12) Пусть E — вещественное гильбертово пространство счетного типа, $\Phi(x, y)$ — скалярное произведение в пространстве E. Показать, что в векторном пространстве E над полем $\boldsymbol{R}$ не существует системы из двух алгебраических базисов (e_λ), (f_μ) таких, что $\Phi(e_\lambda, f_\mu) = \delta_{\lambda\mu}$ для любой пары индексов. Заметить сначала, что множество индексов этих базисов имело бы мощность континуума. (Векторные топологические пространства, гл. II, § 3, упражнение 15); рассмотреть затем (счетный) ортонормальный базис (a_n) пространства E и заметить, что подпространство, порожденное элементами a_n, содержится в подпространстве, порожденном некоторым счетным подмножеством из (e_λ).)

§ 2. Дискриминант полуторалинейной формы

В этом параграфе приняты обозначения: A — коммутативное кольцо, J — антиавтоморфизм кольца A, E — свободный A-модуль конечной размерности n.

Определение 1. *Пусть* Ф — *полуторалинейная относительно* J *форма на модуле* E *и* $S = (x_1, \ldots, x_n)$ — *система из* n *элементов модуля* E. *Дискриминантом формы* Ф *относительно системы* S *называется элемент* $\det(\Phi(x_i, x_j))$ *кольца* A. *Дискриминант формы* Ф *относительно системы* S *обозначается через* $D_\Phi(x_1, \ldots, x_n)$ или $D_\Phi(S)$.

Если $(x_1, \ldots, x_n)$ — *базис* модуля E, то дискриминант формы Ф относительно этого базиса совпадает с определителем матрицы формы Ф относительно этого же базиса.

Из определения продолжения формы Φ на модуль $\bigwedge^n E$ (§ 1, n° 9) следует равенство

$$D_\Phi(x_1, \ldots, x_n) = \Phi_{(n)}(x_1 \wedge \ldots \wedge x_n,\ x_1 \wedge \ldots \wedge x_n), \qquad (1)$$

где $\Phi_{(n)}$ — продолжение формы Φ на $\bigwedge^n E$. Следовательно, для любой перестановки $\sigma \in \mathfrak{S}_n$

$$D_\Phi(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = D_\Phi(x_1, x_2, \ldots, x_n).$$

Пример. Пусть B — *алгебра* над кольцом A, являющаяся свободным A-модулем конечной размерности n. Тогда отображение $(x, y) \to \mathrm{Tr}_{B/A}(xy)$ (гл. VIII, § 12, n° 2) является билинейной формой на B. Пусть задана произвольная система $(x_1, \ldots, x_n)$ n элементов алгебры B; дискриминант этой формы относительно данной системы называется *дискриминантом системы* $(x_1, \ldots, x_n)$ над кольцом A и обозначается через $D_{B/A}(x_1, \ldots, x_n)$. Таким образом,

$$D_{B/A}(x_1, \ldots, x_n) = \det(\mathrm{Tr}_{B/A}(x_i x_j)). \qquad (2)$$

Замечание. Пусть $(e_1, \ldots, e_n)$ — базис алгебры B над кольцом A и $e_i e_j = \sum_{k=1}^{n} c_{ijk} e_k$ — таблица умножения этого базиса (гл. II, § 7, n° 2). Матрица A-линейного эндоморфизма $x \to e_k x$ алгебры B относительно базиса (e_r) равна (c_{ksr}), и поэтому $\mathrm{Tr}_{B/A}(e_k) = \sum_{r=1}^{n} c_{krr}$, откуда $\mathrm{Tr}_{B/A}(e_i e_j) = \sum_{k,\,r} c_{ijk} c_{krr}$. Отсюда следует равенство

$$D_{B/A}(e_1, \ldots, e_n) = \det_{i,\,j}\left(\sum_{k,\,r} c_{ijk} c_{krr}\right). \qquad (3)$$

Предложение 1. *Пусть Φ — форма на модуле E, полуторалинейная относительно J, $(x_1, \ldots, x_n)$ — система n элементов модуля E и $(a_{ij})_{(i,j=1,\ \ldots,\ n)}$ — множество n^2 элементов кольца A; положим $y_j = \sum_{i=1}^{n} a_{ji} x_i$. Тогда выполняется равенство*

$$D_\Phi(y_1, \ldots, y_n) = \det(a_{ij}) \det(a_{ij})^J D_\Phi(x_1, \ldots, x_n).$$

В самом деле, форма Φ полуторалинейна, так что $\Phi(y_i, y_j) = \sum_{k,\,m} a_{ik} \Phi(x_k x_m) a^J_{jm}$. Следовательно, матрица $(\Phi(y_i, y_j))$ равна матрице $A(\Phi(x_i, x_j))\,{}^t A^J$, где $A = (a_{ij})$. Но $\det({}^t A) = \det(A)$ и $\det(A^J) = \det(A)^J$, откуда и следует наше утверждение.

В частности, если (e_i) и (e'_i) — два базиса модуля E, D и D' — дискриминанты формы Φ относительно этих базисов, и a — опре-

делитель матрицы перехода от базиса (e_i) к (e'_i), то справедливо равенство

$$D' = aa^J D. \tag{4}$$

Из предложения 1 следует, что если (e_i)—базис модуля E, то для любой системы $(x_1, \ldots, x_n)$ n элементов E дискриминант $D_\Phi(e_1, \ldots, e_n)$ делит $D_\Phi(x_1, \ldots, x_n)$. В частности, два дискриминанта формы Φ относительно любых двух базисов модуля E порождают один и тот же главный идеал в кольце A.

Пусть $(E_i)_{i\in I}$ — конечное семейство свободных A-модулей конечной размерности, Φ_i — форма на E_i, полуторалинейная относительно J, и B_i — базис модуля E_i. Обозначим через Φ *прямую сумму* форм Φ_i (§ 1, n° 3) и через B — базис модуля $\prod_i E_i$, получающийся объединением базисов B_i; очевидно, имеет место равенство

$$D_\Phi(B) = \prod_{i\in I} D_{\Phi_i}(B_i). \tag{5}$$

Пусть Φ — форма на модуле E, полуторалинейная относительно J, h — гомоморфизм кольца A в коммутативное кольцо A', Φ' — полуторалинейная форма на тензорном произведении $A' \otimes_A E$, получаемая продолжением формы Φ (§ 1, n° 4), и $(x_1, \ldots, x_n)$— произвольная система элементов модуля E. Так как $A' \otimes_A E$ является свободным A'-модулем, определен дискриминант $D_{\Phi'}(1 \otimes x_1, \ldots, 1 \otimes x_n)$ и очевидно равенство

$$D_{\Phi'}(1 \otimes x_1, \ldots, 1 \otimes x_n) = h(D_\Phi(x_1, \ldots, x_n)). \tag{6}$$

Пример. Пусть B — алгебра над кольцом A, являющаяся свободным A-модулем конечной размерности n, $(x_1, \ldots, x_n)$ — базис алгебры B, $\mathfrak{m}$ — идеал кольца A, h — канонический гомоморфизм алгебры B на $B/\mathfrak{m}B$. Тогда система элементов $(h(x_1), \ldots, h(x_n))$ является базисом алгебры $B/\mathfrak{m}B$ над $A/\mathfrak{m}$ (гл. I, § 6, n° 5, предложение 5) и $B/\mathfrak{m}B$ изоморфна $(A/\mathfrak{m}) \otimes_A B$. Следовательно,

$$D_{(B/\mathfrak{m}B)/(A/\mathfrak{m})}(h(x_1), \ldots, h(x_n)) = h(D_{B/A}(x_1, \ldots, x_n)).$$

Предложение 2. *Предположим, что A — кольцо без делителей нуля. Пусть Φ — форма на E, полуторалинейная относительно J, $(e_1, \ldots, e_n)$ — базис модуля E и $D_\Phi(e_1, \ldots, e_n) \neq 0$. Тогда:*

а) *Для того чтобы система $(x_1, \ldots, x_n)$ n элементов модуля E была свободна, необходимо и достаточно, чтобы $D_\Phi(x_1, \ldots, x_n) \neq 0$.*

б) *Для того чтобы система* $(x_1, \ldots, x_n)$ *n элементов модуля* E *была базисом, необходимо и достаточно, чтобы элементы* $D_\Phi(x_1, \ldots, x_n)$ *и* $D_\Phi(e_1, \ldots, e_n)$ *были ассоциированы в кольце* A (ср. гл. VI, § 1, n° 5).

Положим $x_j = \sum_{i=1}^{n} a_{ji}\, e_i$ $(a_{ji} \in A)$. Сначала докажем утверждение а). Если $D_\Phi(x_1, \ldots, x_n) = 0$, то $\det(a_{ji}) \det(a_{ji})^J = 0$ (предложение 1), так как $D_\Phi(e_1, \ldots, e_n) \neq 0$, а кольцо A не имеет делителей нуля. Следовательно, $\det(a_{ji}) = 0$, то есть векторы x_i линейно зависимы (гл. III, § 7, n° 1, теорема 1; применить эту теорему к векторному пространству $K \otimes_A E$, где K — поле дробей кольца A). Обратно, если эти векторы линейно зависимы, то $\det(a_{ji}) = 0$ (там же), откуда $D_\Phi(x_1, \ldots, x_n) = 0$ (предложение 1).

Докажем теперь утверждение б). Если элементы $D_\Phi(x_1, \ldots, x_n)$ и $D_\Phi(e_1, \ldots, e_n)$ ассоциированы в A, то вследствие предложения 1 элемент $\det(a_{ij}) \det(a_{ij})^J$ обратим в кольце A. Точно так же $\det(a_{ij})$ обратим в A, так что матрица (a_{ij}) над кольцом A обратима (гл. III, § 6, n° 5, теорема 2). Поэтому эндоморфизм g модуля E, определенный равенством $g(e_i) = x_i$ $(i = 1, \ldots, n)$, является автоморфизмом; следовательно, система $(x_1, \ldots, x_n)$ является базисом модуля E. Обратное немедленно следует из предложения 1.

Предложение 3. *Пусть* Φ *— полуторалинейная относительно* J *форма на модуле* E. *Следующие условия эквивалентны*:

а) *отображение* s_Φ *модуля* E *в* E^*, *ассоциированное с* Φ, *биективно*;

б) *отображение* d_Φ *модуля* E *в* E^*, *ассоциированное с* Φ, *биективно*;

в) *элемент* $D_\Phi(S)$ *обратим в* A, *где* S *— базис модуля* E.

В самом деле, условие в) означает, что матрица формы Φ относительно базиса S обратима (гл. III, § 6, n° 5, теорема 2). Следовательно, утверждения в) и а) эквивалентны (§ 1, n° 10). Аналогично эквивалентны утверждения в) и б).

Предложение 4. *Пусть* A *— кольцо без делителей нуля, и* S *— базис модуля* E. *Полуторалинейная форма* Φ *на модуле* E *не вырождена тогда и только тогда, когда* $D_\Phi(S) \neq 0$.

В самом деле, пусть K — поле дробей кольца A, Φ' — продолжение формы Φ на векторное K-пространство $K \otimes_A E$; отождествим E с соответствующей частью этого пространства. По формуле (6) условие $D_\Phi(S) \neq 0$ равносильно условию $D_{\Phi'}(S) \neq 0$, которое означает, что отображение $s_{\Phi'}$ биективно (предложение 3), то есть форма Φ' невырождена (§ 1, n° 6, предложение 6). Тогда для любого $x \in K \otimes_A E$ найдется элемент $a \in A$ такой, что $ax \in E$, следовательно, форма Φ будет вырожденной тогда и только тогда, когда вырождена форма Φ'. Это доказывает наше утверждение.

Предложение 5. *Пусть A — поле, B — коммутативная алгебра конечной размерности n над полем A, S — базис алгебры B. Для того чтобы алгебра B была сепарабельной* (гл. VIII, § 7, n° 5, определение 1), *необходимо и достаточно, чтобы* $D_{B/A}(S) \neq 0$.

В самом деле, пусть A' — алгебраическое замыкание поля A, B' — алгебра $A' \otimes_A B$ над A'. Если алгебра B сепарабельна, то алгебра B' полупроста (гл. VIII, § 7, n° 5, следствие предложения 7) и является, следовательно, прямой суммой n полей, изоморфных A' (гл. VIII, § 6, n° 4, следствие предложения 9). Если S' — канонический базис алгебры B' (отождествленной с A'^n), то $D_{B'/A'}(S') = 1$, откуда $D_{B'/A'}(S) \neq 0$ (предложение 1) и $D_{B/A}(S) \neq 0$ (формула (6)).

Обратно, предположим, что $D_{B/A}(S) \neq 0$. Для доказательства сепарабельности алгебры B достаточно показать, что B' полупроста, то есть не содержит нильпотентных элементов, отличных от 0. Но если x' — ненулевой нильпотентный элемент B', то, взяв его в качестве первого элемента базиса S' алгебры B', мы получили бы, что $\mathrm{Tr}_{B'/A'}(x'y') = 0$ для любого $y' \in S'$, так как все собственные значения нильпотентного эндоморфизма равны нулю (гл. VII, § 5, n° 3, следствие 3 предложения 8); следовательно, след равен нулю, но тогда $D_{B'/A'}(S') = 0$, откуда и $D_{B'/A'}(S) = 0$ (предложение 1) и $D_{B/A}(S) = 0$ (формула (6)), что противоречит предположению.

Замечание. Предположим, что B — *надполе* поля A. Пусть $S = (x_1, \ldots, x_n)$ — базис B и $(s_1, \ldots, s_n)$ — A-изоморфизмы надполя B в алгебраическое замыкание A' поля A (каждое s_j повторяется $[B : A]_i$ раз). Напомним, что для любого $z \in B$ выполняется равенство $\mathrm{Tr}_{B/A}(z) = \sum_{j=1}^{n} s_j(z)$ (гл. VIII, § 12, n° 2, предложение 4).

Тогда из формулы умножения определителей следует равенство

$$(\det(s_j(x_i)))^2 = D_{B/A}(x_1, \ldots, x_n). \quad (7)$$

Эта формула показывает, что предложение 5 обобщает условие сепарабельности, приведенное в гл. V, § 7, n° 2, *замечание*.

Предложение 6. *Пусть* Φ *— A-билинейная форма на E, K — такое подкольцо в A, что A является свободным K-модулем конечной размерности q. Пусть* $(e_i)_{i=1, \ldots, n}$ *— базис модуля E над кольцом A и* $(a_j)_{j=1, \ldots, q}$ *— базис модуля A над кольцом K. Тогда* $(a_j e_i)$ *является базисом модуля E над K, отображение* Φ' *произведения $E \times E$ в кольцо K, определенное равенством* $\Phi'(x, y) = \mathrm{Tr}_{A/K}(\Phi(x, y))$, *является K-билинейной формой на модуле E и выполняется равенство*

$$D_{\Phi'}(a_j e_i) = N_{A/K}(D_\Phi(e_1, \ldots, e_n))(D_{A/K}(a_1, \ldots, a_q))^n. \quad (8)$$

Первые два утверждения очевидны, остается доказать равенство (8). По определению, левая часть этого равенства есть определитель K-линейного эндоморфизма u модуля E, заданного формулой

$$u(a_j e_i) = \sum_{r, s} \mathrm{Tr}_{A/K}(a_j a_r \Phi(e_i, e_s)) a_r a_s.$$

Рассмотрим A-линейный гомоморфизм v модуля E, определенный формулой $v(e_i) = \sum_r \Phi(e_i, e_s) e_s$, и K-линейный гомоморфизм w модуля E, определенный формулой $w(a_j e_i) = \left(\sum_r \mathrm{Tr}_{A/K}(a_j a_r) a_r\right) e_i$. Тогда

$$w(v(a_j e_i)) = w\left(\sum_s a_j \Phi(e_i, e_s) e_s\right) = \sum_{r, s} \mathrm{Tr}_{A/K}(a_j \Phi(e_i, e_s) a_r) a_r e_s,$$

поскольку $w(a e_s) = \sum_r \mathrm{Tr}_{A/K}(a a_r) a_r e_s$ для любого $a \in A$; таким образом, u является композицией $w \circ v$. Тогда, обозначив через v_K отображение v, рассматриваемое как K-линейное, будем иметь равенство $\det(u) = \det(v_K) \det(w)$, но $\det(v_K) = N_{A/K}(\det(v))$ (гл. VIII, § 12, n° 2, предложение 7) и, очевидно, $\det(v) = D_\Phi(e_1, \ldots, e_n)$. С другой стороны, каждый из A-модулей Ae_i $(i = 1, \ldots, n)$ устойчив относительно отображения w и определитель сужения w на Ae_i равен $\det(\mathrm{Tr}_{A/K}(a_j a_r)) = D_{A/K}(a_1, \ldots, a_q)$, и поэтому $\det(w) = (D_{A/K}(a_1, \ldots, a_q))^n$. Следовательно, формула (8) сводится к равенству $\det(u) = \det(v_K) \det(w)$, которое уже доказано.

Следствие (формула транзитивности дискриминанта). *Пусть K — коммутативное кольцо, A — коммутативная алгебра с конечным базисом $(a_j)_{j=1, \ldots, q}$ над кольцом K, E — алгебра над A с конечным базисом $(e_i)_{i=1, \ldots, n}$. Тогда $(a_j e_i)$ является базисом алгебры E над кольцом K и*

$$D_{E/K}(a_j e_i) = N_{A/K}(D_{E/A}(e_1, \ldots, e_n))(D_{A/K}(a_1, \ldots, a_q))^n.$$

В самом деле, положив $\Phi(x, y) = \mathrm{Tr}_{E/A}(x, y)$, получим, что форма Φ' из предложения 6 по формуле транзитивности следов (гл. VIII, § 12, n° 2, следствие предложения 7) удовлетворяет равенству $\Phi'(x, y) = \mathrm{Tr}_{E/K}(xy)$.

Упражнения. 1) Пусть A — алгебра конечного ранга с единицей над полем K.

а) Показать, что если радикал алгебры A отличен от нуля, то билинейная форма $(x, y) \to Tr_{A/K}(xy)$ на алгебре A вырождена.

б) Предположим, что поле K имеет характеристику 0. Пусть A — алгебра матриц $\boldsymbol{M}_n(K)$, S — канонический базис алгебры A над полем K. Показать, что $D_{A/K}(S) \neq 0$.

в) Из утверждений а) и б) вывести, что алгебра A конечного ранга над полем характеристики 0 тогда и только тогда абсолютно полупроста, когда билинейная форма $(x, y) \to \mathrm{Tr}_{A/K}(xy)$ не вырождена (или, что то же самое, когда $D_{A/K}(S) \neq 0$ для любого базиса S алгебры A над полем K).

* 2) Пусть B — кольцо и A — его подкольцо, содержащее единицу кольца B; таким образом, B есть (A, A)-*бимодуль*; обозначим через ${}^sB$ (соответственно ${}^dB$) множество B, рассматриваемое как левый (соответственно правый) A-модуль, и через ${}^sB^*$ (соответственно ${}^dB^*$) — правый (соответственно левый) A-модуль, сопряженный к ${}^sB$ (соответственно к ${}^dB$). Если $x' \in {}^sB^*$ и $b \in B$, то отображение $x \to \langle xb, x' \rangle$ будет A-линейной формой на модуле ${}^sB$, то есть элементом модуля ${}^sB^*$; это отображение обозначается через bx'; отображение $(b, x') \to bx'$ определяет на модуле ${}^sB^*$ структуру левого B-модуля (см. гл. III, приложение II, n° 7).

а) Пусть φ — гомоморфизм (A, A)-бимодуля B в (A, A)-бимодуль A; для того чтобы A-билинейное отображение $\Phi : (x, y) \to \varphi(xy)$ произведения ${}^sB \times {}^dB$ в A было невырожденным, необходимо и достаточно, чтобы прообраз $\varphi^{-1}(0)$ не содержал идеалов кольца A, отличных от $\{0\}$ (ни левых, ни правых). В этом случае φ называется *фробениусовым* гомоморфизмом кольца B в подкольцо A.

б) Пусть φ — фробениусов гомоморфизм кольца B в подкольцо A; показать, что отображение d_Φ, ассоциированное с формой Φ справа, является изоморфизмом левого B-модуля ${}^sB$ на некоторый подмодуль левого B-модуля ${}^sB^*$. Показать, что отображение d_Φ биек-

тивно в каждом из двух следующих случаев: 1° A — артиново слева и справа кольцо, удовлетворяющее условиям (N_s) и (N_d) (§ 1, упражнение 11), ${}^sB$ и ${}^dB$ — свободные A-модули конечной длины (использовать упражнение 11б) § 1); 2° A — коммутативное и инволютивное артиново кольцо (гл. VIII, § 3, упражнение 11), содержащееся в центре кольца B, и ${}^sB$ — A-модуль конечной длины (использовать упражнение 11 гл. VIII, § 3).

в) Показать, что, обратно, если модули ${}^sB$ и ${}^sB^*$ изоморфны, то в каждом из случаев, рассмотренных в б), существует фробениусов гомоморфизм кольца B в подкольцо A и модули ${}^sB$ и ${}^dB$ имеют одинаковую длину (использовать упражнение 11б) § 1).

г) В предположениях и обозначениях пункта а) показать, что правый (соответственно левый) аннулятор всякого левого идеала $\mathfrak{l}$ (соответственно правого идеала $\mathfrak{r}$) кольца B есть подмодуль $\mathfrak{l}^0$ (соответственно $\mathfrak{r}^0$), ортогональный относительно формы Φ к подмодулю $\mathfrak{l}$ (соответственно $\mathfrak{r}$) модуля ${}^sB$ (соответственно ${}^dB$).

д) Пусть φ — фробениусов гомоморфизм кольца B в подкольцо A. Показать, что если A — инволютивное артиново кольцо, то при выполнении хотя бы одного из двух условий пункта б) кольцо B также будет инволютивным артиновым кольцом (использовать б) и г)).

3) Пусть A — поле, B — алгебра конечного ранга с единицей над полем A.

а) Для того чтобы алгебра B была фробениусовой, необходимо и достаточно, чтобы существовал фробениусов гомоморфизм алгебры B в A (упражнение 2). (Использовать упражнения 2в) и д) и упражнение 6б) гл. VIII, § 13.)

б) Пусть φ — фробениусов гомоморфизм алгебры B в A; тогда всякая A-линейная форма на алгебре B может быть единственным образом записана в виде $x \to \varphi(b'x)$ (соответственно $x \to \varphi(xb'')$), где b' и b'' принадлежат алгебре B; для того чтобы эта форма была фробениусовой, необходимо и достаточно, чтобы элемент b' (соответственно b'') был обратим в алгебре B.

в) Пусть x^σ для всякого $x \in B$ есть единственный элемент (см. б)) такой, что $\varphi(xy) = \varphi(yx^\sigma)$ для любого $y \in B$. Показать, что отображение $x \to x^\sigma$ является A-автоморфизмом алгебры B. Фробениусова алгебра B называется *симметрической*, если автоморфизм σ внутренний; тогда существует такой фробениусов гомоморфизм алгебры B в A, что автоморфизм σ — тождественный (см. б)), или, что то же самое, (B, B)-бимодули B и ${}^sB^* = {}^dB^*$ (обозначаемый B^*) изоморфны (упражнение 2в)).

г) Пусть E — левый B-модуль конечной длины, E' — его сопряженный модуль и E'^* — модуль, сопряженный к E', рассматриваемый как векторное пространство над полем A; E'^* можно наделить структурой левого B-модуля, положив для любых $x' \in E'$, $x'' \in E'^*$, $b \in B$ $\langle x', bx''\rangle = \langle x'b, x''\rangle$ (гл. III, приложение II, n° 7). Пусть $f_E(x)$ (или

просто $f(x)$), $x \in E$, — элемент модуля E'^* такой, что $\langle x', f(x)\rangle = \varphi(\langle x, x'\rangle)$ для любого $x' \in E'$; показать, что f — биекция левого B-модуля E на левый B-модуль E'^*, полулинейная относительно автоморфизма σ (использовать упражнение 10 гл. VIII, § 4). Если $E = {}^sB$, то (в обозначениях упражнения 2б)) $d_\Phi(x^\sigma) = f_{s_B}(x)$ для всех $x \in B$.

4) а) Пусть G — конечная группа. Показать, что алгебра B группы G над произвольным полем A является симметрической фробениусовой алгеброй (упражнение 3). (Рассмотреть отображение φ алгебры B в A, которое каждому элементу $x = \sum_{s\in G} \xi_s \cdot s$ ставит в соответствие элемент $\varphi(x) = \xi_e$, где e — единица группы G.)

б) Пусть E — векторное пространство конечной размерности n над полем A, и B — внешняя алгебра $\bigwedge E$. Показать, что алгебра B фробениусова. (Пусть $(e_i)_{1\leqslant i\leqslant n}$ — базис пространства E; рассмотреть отображение, которое каждому элементу $x \in B$ ставит в соответствие коэффициент n-вектора $e_1 \wedge e_2 \wedge \ldots \wedge e_n$ в выражении элемента x через базис алгебры B, соответствующий базису (e_i).) Фробениусова алгебра B будет симметрической тогда и только тогда, когда число n четно или поле A имеет характеристику 2.

5) а) Показать, что тензорное произведение двух фробениусовых (соответственно симметрических фробениусовых) алгебр конечного ранга над полем K является фробениусовой (соответственно симметрической фробениусовой) алгеброй (см. § 1, n° 9, предложение 9).

б) Пусть B — алгебра конечного ранга над полем K, L — ее расширение конечной степени над полем K. Показать, что если алгебра $B_{(L)} = B \otimes_K L$ над полем L фробениусова (соответственно симметрическая фробениусова), то алгебра B также фробениусова (соответственно симметрическая фробениусова). (Использовать упражнения 2в) и 3в) и упражнение 2 гл. VIII, § 2.)

6) Показать, что всякая абсолютно полупростая алгебра B конечного ранга над полем K является симметрической фробениусовой алгеброй. (Свести доказательство к случаю, когда алгебра B простая; воспользоваться упражнением 5б), а также предложением 9 гл. VIII, § 12, n° 3.)

§ 3. Эрмитовы и квадратичные формы

В дальнейшем, если не оговорено противное, мы обозначаем через A некоторое кольцо и через E — левый A-модуль. Мы предполагаем, что кольцо A имеет инволютивный антиавтоморфизм J, обозначенный $\alpha \to \bar{\alpha}$; таким образом, $\overline{(\alpha+\beta)} = \bar{\alpha} + \bar{\beta}$, $\overline{(\alpha\beta)} = \bar{\beta}\bar{\alpha}$ и $\bar{\bar{\alpha}} = \alpha$ для любых α, $\beta \in A$. Преполагается, кроме того, что

рассматриваемые полуторалинейные формы, если не оговорено противное, полуторалинейны справа (§ 1, n° 2, определение 4) *относительно этого антиавтоморфизма.*

1. Эрмитовы и ε-эрмитовы формы

Определение 1. *Пусть* ε *— элемент центра кольца* A. *Полуторалинейная форма* Φ *на модуле* E *называется* ε*-эрмитовой, если для любых* $x, y \in E$ *выполнено равенство* $\Phi(x, y) = \varepsilon\Phi(y, x)$. 1*-эрмитова* (соответственно (—1)*-эрмитова*) *форма называется эрмитовой* (соответственно *антиэрмитовой*).

В случае, когда J — тождественный антиавтоморфизм (то есть A обязательно коммутативно), понятие эрмитовой (соответственно антиэрмитовой) формы совпадает с понятием *симметрической* (соответственно *антисимметрической*) билинейной формы (гл. III, § 5, n° 1 , определение 2). Напомним, что знакопеременная билинейная форма (гл. III, § 5, n° 2, определение 4) является антисимметрической; обратное верно, если из равенства $2a = 0$ в кольце A следует, что $a = 0$.

Отношение *ортогональности* (§ 1, n° 3) относительно некоторой ε-эрмитовой формы является, очевидно, *симметричным* (см. упражнение 1).

Если элемент α обратим, то отображение T: $\lambda \to \alpha^{-1}\bar{\lambda}\alpha$ является антиавтоморфизмом кольца и, как легко проверить, форма $\Phi\alpha$ полуторалинейна относительно T. Если, кроме того, $\alpha = \bar{\alpha}$, то T — инволютивный антиавтоморфизм, и если Φ ε-эрмитова, то $\Phi\alpha$ также ε-эрмитова; в самом деле,

$$(\lambda^T)^T = \alpha^{-1}\overline{(\alpha^{-1}\bar{\lambda}\alpha)}\,\alpha = \alpha^{-1}\bar{\alpha}\lambda\bar{\alpha}^{-1}\alpha = \lambda,$$

$$\Phi(y, x)\,\alpha = \varepsilon\overline{\Phi(y, x)}\,\alpha = \varepsilon\,(\Phi(x, y)\,\alpha)^T.$$

В частности, если A — тело, то элементы его центра, удовлетворяющие условию $\bar{\alpha} = \alpha$, образуют в A подполе K, а ε-эрмитовы (относительно J) формы на модуле E образуют векторное пространство над телом K.

Замечания. 1) Если Φ — ε-эрмитова форма на модуле E, то $\Phi(x, y) = \varepsilon\Phi(x, y)\bar{\varepsilon}$ для любых $x, y \in E$. Следовательно, если форма Φ принимает хоть одно обратимое значение, то $\varepsilon\bar{\varepsilon} = 1$.

2) Если в центре кольца A существует элемент i такой, что $\bar{i} = i\varepsilon$, то для того, чтобы форма Φ была ε-эрмитовой, необходимо и достаточно, чтобы форма $i\Phi$ была эрмитовой.

Если отображение $(y, x) \to \overline{\Phi(x, y)}$ полуторалинейно относительно J, то форма Φ будет ε-эрмитовой тогда и только тогда, когда $\Phi(y, x) = \varepsilon\overline{\Phi(x, y)}$ при любых x, y, пробегающих некоторую систему образующих модуля E.

В частности, если E имеет конечный базис $(e_i)_{1\leqslant i\leqslant n}$, то полуторалинейная форма Φ на E ε-эрмитова тогда и только тогда, когда ее матрица $R = (\rho_{ij}) = (\Phi(e_i, e_j))$ удовлетворяет соотношениям $\rho_{ji} = \varepsilon\bar{\rho}_{ij}$ для любых i, j, то есть ${}^tR = \varepsilon\bar{R}$; всякая матрица R, обладающая этим свойством, называется *ε-эрмитовой*. Если $\varepsilon = 1$ (соответственно $\varepsilon = -1$), то R называется *эрмитовой* (соответственно *антиэрмитовой*) относительно автоморфизма J. Если J — тождественный антиавтоморфизм (то есть кольцо A коммутативно), то матрица R эрмитова (соответственно антиэрмитова), если ${}^tR = R$ (соответственно ${}^tR = -R$); тогда говорят, что матрица R *симметрическая* (соответственно *антисимметрическая*).

Для того чтобы форма Φ была знакопеременной, необходимо и достаточно, чтобы ее матрица R была антисимметрической и, кроме того, все диагональные элементы R были равны нулю; всякая матрица, обладающая этими свойствами, называется *знакопеременной*.

Пусть Φ — полуторалинейная форма на модуле E, и s_Φ и d_Φ — ассоциированные с Φ слева и справа отображения модуля E в E^* (§ 1, n° 6). Для того чтобы форма Φ была ε-эрмитова, необходимо и достаточно, чтобы для любых x, $y \in E$ выполнялись равенства $\langle x, s_\Phi(y)\rangle = \bar{\varepsilon}\langle x, d_\Phi(y)\rangle$ и $\langle x, d_\Phi(y)\rangle = \varepsilon\langle x, s_\Phi(y)\rangle$, то есть $s_\Phi = \varepsilon\bar{d}_\Phi$ и $d_\Phi = \varepsilon\bar{s}_\Phi$.

Пусть Φ — ε-эрмитова форма, и ассоциированное с ней справа отображение d_Φ модуля E в E^* биективно. Тогда для всякого эндоморфизма u модуля E

$$u^{**} = \varepsilon\bar{\varepsilon}u. \tag{1}$$

В самом деле, для любых x, $y \in E$ имеем

$$\Phi(x, u^{**}(y)) = \Phi(u^*(x), y) = \varepsilon\overline{\Phi(y, u^*(x))} = \varepsilon\overline{\Phi(u(y), x)} =$$
$$= \varepsilon\Phi(x, u(y))\,\bar{\varepsilon} = \Phi(x, \varepsilon\bar{\varepsilon}u(y)),$$

то есть $u^{**}(x) = \varepsilon\bar{\varepsilon}u(x)$, так как форма Φ невырождена.

Если Φ — ε-эрмитова форма и отображения s_Φ и d_Φ биективны, то ее *обратная форма* $\hat{\Phi}$ (§ 1, n° 7) *является* $\bar{\varepsilon}$*-эрмитовой формой*. В самом деле, положив для краткости $s = s_\Phi$, $d = d_\Phi$, из условия $d = \varepsilon s$ получим $s^{-1} = \bar{\varepsilon} d^{-1}$, так как s полулинейно. Далее, для любых $u, v \in E$ имеем

$$\hat{\Phi}(u, v) = \Phi(s^{-1}(u),\ d^{-1}(v)) = \bar{\varepsilon}\Phi(d^{-1}(u),\ d^{-1}(v)),$$

откуда $\hat{\Phi}(v, u) = \bar{\varepsilon}\varepsilon\overline{\Phi(d^{-1}(u),\ d^{-1}(v))} = \varepsilon\overline{\hat{\Phi}(u, v)}$, так как ε входит в центр кольца A.

Наконец, в случае, когда кольцо A коммутативно, канонические продолжения ε-эрмитовой формы Φ на тензорные и внешние степени $\overset{p}{\otimes} E$ и $\overset{p}{\bigwedge} E$ являются ε-эрмитовыми формами. Это немедленно следует из формул (35) и (37) § 1, n° 9.

2. *Модули над квадратичным расширением*

Пусть K — коммутативное кольцо, $A = K(i)$ — его квадратичное расширение, $i^2 = -1$ и J — автоморфизм $\lambda + i\mu \to \lambda - i\mu$ ($\lambda \in K$, $\mu \in K$) (гл. II, § 7, n° 7).

Взяв A-модуль E, обозначим через E_0 K-модуль, получаемый из модуля E сужением кольца скаляров, а через j — автоморфизм $x \to ix$ модуля E_0; очевидно, $j^2 = -I$, где I — тождественное отображение модуля E_0. Обратно, пусть E_0 — K-модуль и j — его автоморфизм такой, что $j^2 = -I$; тогда отображение $\lambda + i\mu \to \lambda I + \mu j$ является, очевидно, гомоморфизмом кольца A в кольцо $\mathscr{L}(E_0)$ эндоморфизмов модуля E_0; следовательно, на E_0 определена структура A-модуля, для которой

$$(\lambda + i\mu)x = \lambda x + \mu j(x) \qquad (x \in E_0 \lambda \in K,\ \mu \in K). \tag{2}$$

Пусть E' — еще один A-модуль, E'_0 — соответствующий K-модуль, j' — автоморфизм $x' \to ix'$ модуля E'_0; тогда A-линейные отображения f модуля E в E' представляют собой не что иное, как K-линейные отображения модуля E_0 в E'_0, удовлетворяющие соотношению $f \circ j = j' \circ f$. В частности, если заданы два отображения f_1 и f_2 модуля E в K, то отображение $x \to f_1(x) + f_2(x)$ модуля E в A будет A-линейным тогда и только тогда, когда f_1 и f_2 принадлежат сопряженному модулю E^* и $f_1 \circ j + i(f_2 \circ j) = if_1 - f_2$, то есть $f_1 = f_2 \circ j$ и $f_1 \circ j = -f_2$. Эти два условия

эквивалентны, так как j — автоморфизм модуля E_0 и $j^2 = -I$. Исключая одно из отображений, f_1 или f_2, получим, что формулы

$$f(x) = f_1(x) - if_1(j(x)), \tag{3}$$

$$f(x) = f_2(j(x)) + if_2(x) \tag{4}$$

($x \in E$, $f \in E^*$, $f_1 \in (E_0)^*$, $f_2 \in (E_0)^*$) устанавливают взаимно однозначное соответствие между сопряженными модулями E^* и $(E_0)^*$

3. *Билинейные формы, ассоциированные с эрмитовой формой*

Мы сохраняем здесь предположение, что A является *квадратичным расширением* $A = K(i)$ (где $i^2 = -1$) коммутативного кольца K и J — автоморфизм $\lambda + i\mu \to \lambda - i\mu$ ($\lambda \in K$, $\mu \in K$) этого кольца. Пусть E и E' — A-модули, E_0 и E'_0 — соответствующие K-модули, j и j' — автоморфизмы $x \to ix$ и $x' \to ix'$ модулей E_0 и E'_0 (ср. n° 2). K-билинейная форма f на произведении $E_0 \times E'_0$ называется *инвариантной относительно автоморфизмов* j и j', если для любых $x \in E_0$ и $x' \in E'_0$

$$f(j(x), j'(x')) = f(x, x'). \tag{5}$$

Заменяя здесь x на $j(x)$, получим, что это условие эквивалентно выполнению равенства

$$f(x, j'(x')) = -f(j(x), x') \tag{6}$$

для любых $x \in E_0$ и $x' \in E'_0$.

Предложение 1. *Пусть* Φ_1 (соответственно Φ_2) — *K-билинейная форма на произведении* $E_0 \times E'_0$, *инвариантная относительно* j *и* j'. *Отображение, которое форме* Φ_1 (соответственно Φ_2) *ставит в соответствие отображение* Φ *произведения* $E \times E'$ *в кольцо* A, *определенное формулой*

$$\Phi(x, x') = \Phi_1(x, x') + i\Phi_1(x, j(x')) \tag{7}$$

(соответственно $\Phi(x, x') = -\Phi_2(x, j(x')) + i\Phi_2(x, x')$) (8)

($x \in E$, $x' \in E'$), *является изоморфизмом векторного K-пространства K-билинейных форм на произведении* $E_0 \times E'_0$, *инвариантных относительно* j *и* j', *на векторное K-пространство полуторалинейных форм на произведении* $E \times E'$. *Если, кроме того,* $E = E'$,

то форма Φ *эрмитова тогда и только тогда, когда форма* Φ_1 *симметрична* (соответственно *форма* Φ_2 *антисимметрична*) (см. упражнение 4).

В самом деле, всякое отображение Φ произведения $E \times E'$ в кольцо A можно однозначно записать в виде $\Phi = \Phi_1 + i\Phi_2$, где Φ_1 и Φ_2 — отображения произведения $E \times E'$ в кольцо K. В силу формулы (3) (соответственно (4)) n° 2, для того чтобы отображение $x \to \Phi(x, x')$ было A-линейным, необходимо и достаточно, чтобы форма Φ_1 (соответственно Φ_2) была K-линейна по x и удовлетворялось соотношение

$$\Phi(x, x') = \Phi_1(x, x') - i\Phi_1(j(x), x') \tag{9}$$

$$(\text{соответственно } \Phi(x, x') = -\Phi_2(j(x), x') + i\Phi_2(x, x')). \tag{10}$$

Аналогично, для того чтобы отображение $\overline{\Phi(x, x')}$ было A-линейно по x', необходимо и достаточно, чтобы отображение Φ_1 (соответственно Φ_2) было K-линейно по x' и удовлетворялось соотношение

$$\Phi(x, x') = \Phi_1(x, x') + i\Phi_1(x, j'(x')) \tag{11}$$

$$(\text{соответственно } \Phi(x, x') = -\Phi_2(x, j'(x') + i\Phi_2(x, x'))). \tag{12}$$

Отсюда немедленно следует, что отображение Φ полуторалинейно тогда и только тогда, когда оно может быть записано в виде (9) или (11) (соответственно (10) или (12)), где K-билинейная форма Φ_1 (соответственно Φ_2) инвариантна относительно автоморфизмов j и j'.

Отсюда следует, что для того, чтобы полуторалинейная форма $\Phi = \Phi_1 + i\Phi_2$ была нулевой, необходимо и достаточно, чтобы форма Φ_1 (соответственно Φ_2) была нулевой. Наконец, если $E = E'$, то $\Phi(y, x) = \Phi_1(y, x) + i\Phi_2(y, x)$ и $\overline{\Phi(x, y)} = \Phi_1(x, y) - i\Phi_2(x, y)$, и для того, чтобы эти два выражения совпадали, или, что то же, форма Φ была эрмитовой, необходимо и достаточно, чтобы форма Φ_1 была симметрической (соответственно форма Φ_2 была антисимметрической).

Замечания. 1) Формулы (7) и (8) показывают, что при $x \in E$ равенство $\Phi(x, x') = 0$ выполняется для любого $x' \in E'$ тогда и только тогда, когда $\Phi_1(x, x') = 0$ (соответственно $\Phi_2(x, x') = 0$) для всех $x' \in E'$.

2) Пусть u — эндоморфизм модуля E; сопряженный с ним относительно Ф эндоморфизм (§ 1, n° 8) совпадает с сопряженным относительно Φ_1 (соответственно Φ_2) эндоморфизмом (если рассматривать u как эндоморфизм модуля E_0).

4. Квадратичные формы

Определение 2. *Пусть кольцо A коммутативно. Отображение Q модуля E в кольцо A называется квадратичной формой на модуле E, если*

1) $Q(\alpha x) = \alpha^2 Q(x)$ *для* $\alpha \in A$ *и* $x \in E$;

2) *отображение* Φ: $(x, y) \to Q(x + y) - Q(x) - Q(y)$ *произведения* $E \times E$ *в кольцо* A *является билинейной формой.*

Билинейная форма Φ (*непременно симметрическая*) *называется билинейной формой, ассоциированной с формой* Q.

Если форма Φ *невырождена, то и форма* Q *называется невырожденной.*

Так как $Q(2x) = 4Q(x)$, то из условия 2) сразу следует равенство

$$\Phi(x, x) = 2Q(x). \tag{13}$$

Если, в частности, характеристика кольца A равна 2, то форма Φ *знакопеременная.*

Два элемента (соответственно два подмножества) модуля E будем называть *ортогональными* относительно квадратичной формы Q, если они ортогональны относительно ассоциированной с Q билинейной формы Φ.

Пусть $(x_i)_{i \in I}$ — семейство элементов модуля E, и $(a_i)_{i \in I}$ — семейство элементов кольца A, лишь конечное число которых отлично от нуля. Индукцией по числу i индексов, для которых $a_i \neq 0$, легко доказать равенство

$$Q\left(\sum_i a_i x_i\right) = \sum_i a_i^2 Q(x_i) + \sum_{\{i, j\}} a_i a_j \Phi(x_i, x_j), \tag{14}$$

в котором последняя сумма распространяется на двухэлементные *подмножества* множества I.

Для всякой билинейной формы f на произведении $E \times E$ можно определить квадратичную форму Q, положив $Q(x) = f(x, x)$; тогда билинейная форма Φ, ассоциированная с Q, определяется равенством $\Phi(x, y) = f(x, y) + f(y, x)$ для любых

$x, y \in E$. Более того, если скаляр 2 имеет обратный $\frac{1}{2}$ в кольце A, то существует единственная *симметрическая* билинейная форма f, удовлетворяющая равенству $Q(x) = f(x, x)$, именно $\frac{1}{2}\Phi$; дискриминант формы f относительно системы $S = (x_1, \ldots, x_n)$ называется также дискриминантом формы Q относительно системы S. Таким образом, в этом случае существует взаимно однозначное соответствие между квадратичными формами и симметрическими билинейными формами на модуле E (см. упражнение 6).

Если модуль E свободен, то справедливо, кроме того, следующее утверждение:

Предложение 2. *Пусть кольцо A коммутативно и модуль E обладает некоторым базисом $(e_i)_{i\in I}$. Тогда для всякой квадратичной формы Q на модуле E на произведении $E \times E$ существует билинейная форма f такая, что $Q(x) = f(x, x)$ для любого $x \in E$. Для любого множества $(b_{ij})_{(i,j)\in I\times I}$ скаляров таких, что $b_{ij} = b_{ji}$ для $(i, j) \in I \times I$, существует единственная квадратичная форма, удовлетворяющая равенствам*

$$Q(e_i) = b_{ii},\ \Phi(e_i, e_j) = b_{ij} \quad \text{для} \quad i \neq j, \tag{15}$$

где Φ — билинейная форма, ассоциированная с Q; форма Q определяется формулой

$$Q\Big(\sum_i a_i e_i\Big) = \sum_{\{i,j\}} b_{ij} a_i a_j, \tag{16}$$

где сумма распространяется на подмножества $\{i, j\}$ множества I, содержащие один или два элемента.

В самом деле, формула (16) является лишь новой записью для (14), откуда следует единственность квадратичной формы Q, удовлетворяющей равенству (15). Чтобы доказать ее существование, заметим прежде всего, что в кольце A существует множество (b'_{ij}) такое, что $b'_{ii} = b_{ii}$ и $b'_{ij} + b'_{ji} = b_{ij}$ при $i \neq j$; такое множество можно получить, наделив множество I структурой совершенно упорядоченного множества (Теор. мн., гл. III, § 3, n° 3, теорема 1) и положив $b'_{ij} = b_{ij}$ для $i < j$ и $b'_{ij} = 0$ для $i > j$. Так как элементы e_i образуют базис модуля E, то существует билинейная форма f на произведении $E \times E$, удовлетворяющая равенству $f(e_i, e_j) = b'_{ij}$; положив $Q'(x) = f(x, x)$ и обозначив

через Φ' билинейную форму, ассоциированную с квадратичной формой Q', будем иметь равенства $Q'(e_i) = b_{ii}$ и $\Phi'(e_i, e_j) = f(e_i, e_j) + f(e_j, e_i) = b_{ij}$. Это доказывает второе наше утверждение. Что же касается первого утверждения, то оно немедленно следует из предыдущего рассуждения, так как, в силу единственности, если квадратичная форма Q удовлетворяет равенству (15), то $Q(x) = Q'(x) = f(x, x)$.

Модуль E, наделенный структурой, определяемой квадратичной формой Q, будем называть *квадратичным модулем*. Гомоморфизм квадратичного модуля (E, Q) в квадратичный модуль (E', Q') — это такое линейное отображение u модуля E в E', что $Q = Q' \circ u$; если Φ и Φ' — ассоциированные с Q и Q' билинейные формы, то для $x \in E$, $y \in E$ выполняется равенство $\Phi(x, y) = \Phi'(u(x), u(y))$; иными словами, форма Φ' является обратным образом формы Φ относительно гомоморфизма u (§ 1, n° 1). Две квадратичные формы Q и Q' на A-модулях E и E' называются эквивалентными, если соответствующие квадратичные модули изоморфны.

Пусть $(E_i, Q_i)_{i \in I}$ — множество квадратичных модулей, и E — прямая сумма модулей E_i. *Внешней прямой суммой квадратичных модулей* (E_i, Q_i) назовем квадратичный модуль, получающийся при наделении модуля E квадратичной формой Q, определяемой равенством $Q(\sum_i x_i) = \sum_i Q_i(x_i)$ для $x_i \in E_i$. Форму Q также называют *внешней прямой суммой* квадратичных форм Q_i.

Если все формы Q_i невырождены, то форма Q также невырождена.

Пусть Q — квадратичная форма на A-модуле E, F — подмодуль модуля E. Предположим, что форма Q постоянна на каждом классе по модулю F. Тогда получаемое путем факторизации из Q отображение $\overline{Q}$ модуля E/F в кольцо A будет, очевидно, квадратичной формой, а каноническое отображение модуля E на E/F будет гомоморфизмом структур квадратичных модулей. Для того чтобы форма Q была постоянной на каждом классе по модулю F, необходимо и достаточно, чтобы для любых $x \in E$ и $y \in F$ выполнялось равенство $Q(x+y) = Q(x)$, то есть $Q(y) + \Phi(x, y) = 0$, где Φ — ассоциированная с Q билинейная форма. Положив здесь $x = 0$, получим, что $Q(y) = 0$ для любого $y \in F$, и следовательно, $\Phi(x, y) = 0$ для $x \in E$ и $y \in F$. Множество N элемен-

тов x модуля E таких, что $Q(x) = 0$ и $\Phi(x, z) = 0$ для любого $z \in E$, называется *ядром* квадратичного модуля (E, Q). Таким образом, для того чтобы форма Q была постоянной на каждом классе по модулю F, необходимо и достаточно, чтобы подмодуль F содержался в ядре N модуля (E, Q). Легко проверить, что ядро N является в E подмодулем. Следовательно, для того чтобы форма Q была постоянной на каждом классе по модулю F, необходимо и достаточно, чтобы подмодуль F был порожден элементами ядра N.

Легко видеть, что ядро квадратичного модуля E/N равно $\{0\}$.

Предложение 3. *Пусть h — гомоморфизм кольца A в коммутативное кольцо A'. Для всякой квадратичной формы Q на A-модуле E существует единственная квадратичная форма Q' на A'-модуле $A' \otimes_A E$* (гл. III, приложение II, n° 10), *удовлетворяющая условию*

$$Q'(1 \otimes x) = h(Q(x)) \tag{17}$$

для любого $x \in E$. Кроме того, билинейная форма Φ', ассоциированная с Q', получается из билинейной формы Φ, ассоциированной с Q, расширением кольца скаляров.

Покажем прежде всего, что если квадратичная форма Q', удовлетворяющая равенству (17), существует, то она единственна, и билинейная форма Φ', ассоциированная с Q', получается из билинейной формы Φ, ассоциированной с Q, расширением кольца скаляров. В самом деле, последнее утверждение следует из того, что для любых $x \in E$, $y \in E$ выполняется равенство

$$\Phi'(1 \otimes x,\ 1 \otimes y) = Q'(1 \otimes x + 1 \otimes y) - Q'(1 \otimes x) - Q'(1 \otimes y) = \\ = h(\Phi(x, y)). \tag{18}$$

Тогда из формулы (14) следует, что

$$Q'\Big(\sum_i a'_i \otimes x_i\Big) = \sum_i a'^2_i h(Q(x_i)) + \sum_{\{i,j\}} a'_i a'_j h(\Phi(x_i, x_j)) \tag{19}$$

для любых $a'_i \in A'$ и $x_i \in E$, откуда и вытекает единственность формы Q'.

Чтобы доказать существование формы Q', предположим сначала, что модуль E имеет некоторый базис $(e_i)_{i \in I}$. Тогда в кольце A существуют элементы b_{ij} такие, что $b_{ij} = b_{ji}$ и $Q\big(\sum_i a_i e_i\big) =$

$= \sum_{\{i,j\}} b_{ij}a_ia_j$ для $a_i \in A$ (предложение 2). Элементы $1 \otimes_A e_i$ образуют базис A'-модуля $A' \otimes_A E$, и поэтому, положив для $a'_i \in A'$

$$Q'\left(\sum_i a'_i \otimes e_i\right) = \sum_{\{i,j\}} a'_i a'_j h(b_{ij}), \tag{20}$$

мы получим квадратичную форму Q' на этом модуле; отсюда при $x = \sum_i a_i e_i \in E$ выполняется равенство

$$Q'(1 \otimes x) = Q'\left(\sum_i h(i) \otimes e_i\right) = \sum_{\{i,j\}} h(a_i)\,h(a_j)\,h(b_{ij}) = h(Q(x)), \tag{21}$$

что и доказывает существование формы Q' в рассматриваемом случае.

Перейдем теперь к общему случаю. Пусть $(x_i)_{i\in I}$ — система образующих модуля E, $A^{(1)}$ — модуль формальных линейных комбинаций элементов множества I (гл. II, § 1, n° 8) и $(e_i)_{i\in I}$ — канонический базис модуля $A^{(1)}$. Поскольку элементы x_i порождают модуль E, то отображение u модуля $A^{(1)}$ в E, определенное формулой $u(e_i) = x_i$, сюръективно. Отсюда следует (гл. III, приложение II, n° 5, предложение 4), что отображение $1 \otimes u$ модуля $A' \otimes A^{(1)}$ в $A' \otimes E$ сюръективно и его ядро p' порождается элементами вида $1 \otimes p$, где $u(p) = 0$. Обозначим через Q'_1 продолжение на модуль $A' \otimes_A A^{(1)}$ квадратичной формы $Q_1 = Q \circ u$ на модуле $A^{(1)}$. Если элемент $p \in A^{(1)}$ удовлетворяет условию $u(p) = 0$, то $Q'_1(1 \otimes p) = h(Q_1(p)) = 0$ и для любого $x \in A^{(1)}$ $\Phi'_1(1 \otimes p,\ 1 \otimes x) = h(\Phi(u(p), u(x)))$, где Φ'_1 — билинейная форма, ассоциированная с Q'_1. Таким образом, если $u(p) = 0$ $(p \in A^{(1)})$, то элемент $1 \otimes p$ входит в ядро квадратичного модуля $A' \otimes_A A^{(1)}$ и, как мы видели выше, на произведении $A' \otimes_A E$ существует квадратичная форма Q' такая, что $Q'_1 = Q' \circ (1 \otimes u)$. Но отображение u сюръективно, так что форма Q' удовлетворяет условию (17), что и требовалось доказать.

Квадратичная форма Q', существование и единственность которой установлены в предложении 3, называется продолжением формы Q на произведение $A' \otimes_A E$ (относительно гомоморфизма h). Говорят также, что форма Q' получается из формы Q расширением кольца скаляров.

Упражнения. 1) Пусть A — тело, E — левое векторное пространство над A, Φ — полуторалинейная форма на E (относи-

тельно некоторого антиавтоморфизма J тела A). Предположим, что ранг формы Φ (конечный или бесконечный) $\geqslant 2$ и что равенства $\Phi(x, y) = 0$ и $\Phi(y, x) = 0$ *эквивалентны*.

а) Показать, что в A существует элемент $\lambda \neq 0$ такой, что $\Phi(y, x) = \lambda(\Phi(x, y))^J$ (воспользоваться упражнением 8 к § 1).

б) Показать, что существует $\alpha \in A$ такой, что полуторалинейная (относительно антиавтоморфизма $\xi \to \alpha^{-1}\xi^J\alpha$) форма $\Phi\alpha$ эрмитова или знакопеременна. (Заметить прежде всего, что $\xi^{J^2} = \lambda^{-1}\xi^J\lambda^{-1}$ и $\lambda\lambda^J = \lambda^J\lambda = 1$, и рассмотреть два случая: $\xi + \xi^J\lambda^{-1} = 0$ для любого $\xi \in A$ или нет; во втором случае показать, что всякий отличный от нуля элемент вида $\alpha = \xi + \xi^J\lambda^{-1}$ удовлетворяет требуемому условию.)

2) Пусть Φ — ε-эрмитова полуторалинейная форма на векторном пространстве E конечной размерности над полем A.

а) Показать, что для всякого векторного подпространства M пространства E выполняются равенства $(M^0)^0 = M + E^0$ и $\dim M^0 + \dim M = \dim E + \dim(M \cap E^0)$.

б) Показать, что для любых подпространств M_1 и M_2 пространства E справедливо равенство $\dim(M_1 \cap M_2^0) + \dim(M_2 + M_1^0) = \dim E + \dim(M_1 \cap E^0)$ (рассмотреть каноническое отображение пространства E на E/E^0).

3) Пусть K — коммутативное кольцо, $f \in K[X]$ — унитарный многочлен степени $n \geqslant 1$; пусть A — факторалгебра $K[X]/f$ с базисом $1, \xi, \xi^2, \ldots, \xi^{n-1}$ над кольцом K (гл. IV, § 1, n° 5, предложение 4). Показать, что задание A-модуля E равносильно заданию K-модуля E_0 и K-эндоморфизма j модуля E_0 такого, что $f(j) = 0$. Для любого $u \in E^*$ положим $u(x) = \sum_{k=0}^{n-1} u_k(x)\,\xi^k$; показать, что если элемент $\alpha_0 = f(0)$ обратим в кольце K, то отображение $u \to u_0$ является K-изоморфизмом модуля E^* на $(E_0)^*$, который называется обратным изоморфизмом.

*4) а) Пусть A — кольцо (коммутативное или нет), σ — автоморфизм кольца A, для которого существует обратимый элемент $\gamma \in A$, удовлетворяющий условию $\gamma^\sigma = \gamma$, и пусть для любого $\xi \in A$ справедливо равенство $\xi^{\sigma^2} = \gamma\xi\gamma^{-1}$. Пусть B — левый A-модуль с базисом из двух элементов (e_1, e_2); показать, что закон композиции

$$(\xi e_1 + \eta e_2)(\xi' e_1 + \eta' e_2) = (\xi\xi' + \eta\eta^\sigma\gamma)\,e_1 + (\eta\xi'^\sigma + \xi\eta')\,e_2$$

определяет на модуле B структуру кольца.

Элемент e_1 является единичным элементом для этой структуры кольца (и отождествляется с единицей 1 кольца A); если e_2 обозначить через ϱ, то будут выполняться равенства $\varrho^2 = \gamma$ и $\varrho\xi = \xi^\sigma\varrho$ для любого $\xi \in A$; кроме того, B является правым A-модулем с базисом 1 и ϱ. Если A — тело, то кольцо B будет телом тогда и только

тогда, когда элемент γ не представим в виде $\lambda^\sigma\lambda$ (где $\lambda \in A$) (см. гл. VIII, § 12, упражнение 8).

б) Пусть J — инволютивный антиавтоморфизм кольца A. Предположим, что существует обратимый элемент $\delta \in A$, удовлетворяющий следующим условиям:

$$\delta^J = \delta, \quad \delta^\sigma\delta = \gamma\gamma^J, \quad (\xi^J)^\sigma = \delta(\xi^\sigma)^J\delta^{-1} \text{ для любого } \xi \in A. \tag{1}$$

Показать, что, положив

$$(\xi+\eta\varrho)^J = \xi^J + \gamma^{-1}\delta^\sigma(\eta^J)^\sigma\varrho, \tag{2}$$

антиавтоморфизм J можно продолжить до инволютивного антиавтоморфизма кольца B (также обозначаемого через J).

Предположим дополнительно, что A и B — тела и антиавтоморфизм J не внутренний. Показать, что условия (1) необходимы для существования продолжения антиавтоморфизма J до инволютивного антиавтоморфизма тела B (положив $\varrho^J = \alpha + \beta\varrho$, где $\alpha, \beta \in A$, показать, что при выполнении условия $(\varrho\xi)^J = \xi^J\varrho^J$ для всех $\xi \in A$ должно быть $\alpha = 0$).

в) Предположим, что условия (1) выполнены и что инволютивный антиавтоморфизм J продолжен на кольцо B по формуле (2). Пусть F — унитарный B-модуль, E — унитарный A-модуль, полученный из модуля F сужением кольца скаляров до A; тогда отображение $j : x \to \varrho x$ является биективным отображением модуля E на себя, полулинейным относительно автоморфизма σ кольца A, и выполняется равенство $j^2(x) = \gamma x$. Пусть Φ — эрмитова форма на модуле F (относительно J); для $x \in E$, $y \in E$ положим $\Phi(x, y) = \Phi_1(x, y) + \Phi_2(x, y)\varrho$, где $\Phi_1(x, y) \in A$, $\Phi_2(x, y) \in A$. Показать, что Φ_1 — эрмитова форма на модуле E (относительно J) и

$$\Phi_1(j(x), j(y)) = (\Phi_1(x, y))^\sigma\delta.$$

Далее, $\Phi_2(x, y) = \Phi_1(x, j(y))\,\delta^{-1}$, Φ_2 — форма на модуле E, полуторалинейная относительно антиавтоморфизма $\xi \to (\xi^J)^\sigma$ (вообще говоря, не инволютивного), и выполняются равенства

$$\Phi_2(j(x), j(y)) = \Phi_2(x, y))^\sigma\delta^\sigma$$

и

$$\Phi_2(y, x) = \gamma^J\delta^{-1}((\Phi_2(x, y))^J)^\sigma.$$

Обратно: для того чтобы форма Φ была невырождена, необходимо и достаточно, чтобы были невырождены формы Φ_1 и Φ_2. Частный случай: B — алгебра кватернионов над коммутативным кольцом K, соответствующая паре (α, β) элементов кольца K, где β — обратимый элемент, A — подалгебра $K + Ku$ алгебры B, J и σ — отображения $\xi \to \bar{\xi}$ (гл. II, § 7, n° 8).

г) Пусть u — автоморфизм A-модуля E. Для того чтобы u был автоморфизмом B-модуля F, оставляющим инвариантной форму Φ,

необходимо и достаточно, чтобы он удовлетворял двум из следующих трех условий:

1° u оставляет инвариантной форму Φ_1;

2° u оставляет инвариантной форму Φ_2;

3° u перестановочен с j.

5) Пусть A — коммутативное кольцо, E — A-модуль, $(x_i)_{i\in I}$ — система образующих модуля E; пусть R — подмодуль модуля $A^{(I)}$, состоящий из элементов $(y_i)_{i\in I}$ таких, что $\sum_i y_i x_i = 0$, и пусть $(a_\lambda)_{\lambda\in L}$ — система образующих подмодуля R (здесь $a_\lambda = (a_{\lambda i})_{i\in I}$). Пусть (b_{ij}) — некоторое семейство элементов кольца A ($i \in I$, $j \in I$). Для того чтобы существовала квадратичная форма Q такая, что $Q(x_i) = b_{ii}$ и $\Phi(x_i, x_j) = b_{ij}$ при $i \neq j$ (Φ — ассоциированная с Q билинейная форма), необходимо и достаточно, чтобы $b_{ij} = b_{ji}$ для любых $i, j \in I$ и для любых $\lambda \in L$ и $i \in I$ выполнялось равенство

$$\sum_{\{i,j\}} b_{ij}a_{\lambda i}b_{\lambda j} = \sum_{j\neq i} b_{ij}a_{\lambda j} + 2b_{ii}a_{\lambda i} = 0. \qquad (3)$$

Тогда $Q(\sum_i a_i x_i) = \sum_{\{i,j\}} b_{ij}\, a_i a_j$. Вывести отсюда новое доказательство предложения 3 n° 4. (Заметить, что элементы $x'_i = 1 \otimes x_i$ составляют систему образующих модуля $A' \otimes_A E$ и что A'-модуль $A' \otimes_A E$ изоморфен $A'^{(I)}/R'$, где $A'^{(I)}$ отождествлен с $A' \otimes_A A^{(I)}$, а R' порождается образом подмодуля R при каноническом отображении модуля $A^{(I)}$ в $A'^{(I)}$.)

6) Пусть A — коммутативное кольцо характеристики 2, E — свободный A-модуль, $\mathscr{H}$ (соответственно $\mathscr{G}$, $\mathscr{D}$) — A-модуль знакопеременных билинейных (соответственно симметрических билинейных, квадратичных) форм на модуле E. Тогда $\mathscr{H} \subset \mathscr{G}$; следующим образом определим линейные отображения ω модуля $\mathscr{G}$ в $\mathscr{D}$ и ϑ — модуля $\mathscr{D}$ в $\mathscr{H}$: для любой билинейной формы $\Phi \in \mathscr{G}$ $\omega(\Phi)$ есть квадратичная форма $x \to \Phi(x, x)$, и для любой квадратичной формы $Q \in \mathscr{D}$ $\vartheta(Q)$ есть билинейная форма, ассоциированная с Q; эта форма знакопеременная. Показать, что $\omega^{-1}(0) = \mathscr{H}$, $\vartheta(\mathscr{D}) = \mathscr{H}$ и $\vartheta^{-1}(0) = \omega(\mathscr{G})$.

*7) Пусть A — коммутативное кольцо, E, F — A-модули. Отображение Q модуля E в F называется *квадратическим*, если выполняются следующие условия: 1° $Q(\alpha x) = \alpha^2 Q(x)$ для $\alpha \in A$, $x \in E$; 2° отображение $(x, y) \to Q(x + y) - Q(x) - Q(y)$ произведения $E \times E$ в F билинейно. Если отображение f A-модуля E_1 в E линейно, то композиция $Q \circ f$ является квадратическим отображением модуля E_1 в F.

а) Пусть E — A-модуль, $A^{(E)}$ — модуль формальных линейных комбинаций элементов модуля E с коэффициентами из кольца A (гл. II,

§ 1, п° 8) и для любого $x \in E$ ε_x — элемент канонического базиса модуля $A^{(E)}$, соответствующий x. Пусть $\Gamma^2(E)$ — фактормодуль модуля $A^{(E)} \times (E \otimes_A E)$ по подмодулю R, порожденному элементами $(\varepsilon_{x+y} - \varepsilon_x - \varepsilon_y,\ -x \otimes y)$ и $(\varepsilon_{\lambda x} - \lambda^2 \varepsilon_x,\ 0)$, $x \in E$, $y \in E$, $\lambda \in A$. Положим для любого $x \in E$ $\gamma(x) = \varphi(\varepsilon_x,\ 0)$, где φ — каноническое отображение модуля $A^{(E)} \times (E \otimes E)$ на $\Gamma^2(E)$, γ называется *каноническим отображением* модуля E в $\Gamma^2(E)$. Доказать, что γ — квадратическое отображение модуля E в $\Gamma^2(E)$ и что для любого квадратического отображения Q модуля E в A-модуль F существует единственное *линейное* отображение q модуля $\Gamma^2(E)$ в F такое, что $Q = q \circ \gamma$ (другими словами, пара $(\Gamma^2(E), \gamma)$ является решением проблемы универсального отображения; см. Теор. мн., гл. IV, § 3).

Показать, что для любых A-модулей E и E' любого линейного отображения f модуля E в E' существует единственное линейное отображение $\overline{f}$ модуля $\Gamma^2(E)$ в $\Gamma^2(E')$ такое, что $\gamma' \circ f = \overline{f} \circ \gamma$, где γ' — каноническое отображение модуля E' в $\Gamma^2(E')$.

б) Предположим, что модуль E является прямой суммой двух подмодулей M и N. Определить канонический изоморфизм модуля $\Gamma^2(E)$ на прямую сумму модулей $\Gamma^2(M)$, $\Gamma^2(N)$ и $M \otimes N$ (показать, что эта прямая сумма является решением той же проблемы универсального отображения, что и $\Gamma^2(E)$).

в) Пусть F — подмодуль в E, j — каноническая инъекция модуля F в E. Определить канонический изоморфизм модуля $\Gamma^2(E/F)$ на

$$\Gamma^2(E)/(\overline{j}(\Gamma^2(F)) + \psi(E \times F)),$$

где $\psi(x, y) = \varphi(0, x \otimes j(y))$ для $x \in E$, $y \in F$. (Тем же способом, что и в предыдущем упражнении.)

г) Пусть A' — коммутативное кольцо, h — гомоморфизм кольца A в A'. Определить канонический изоморфизм модуля $\Gamma^2(A' \otimes_A E)$ на $A' \otimes_A \Gamma^2(E)$ (тем же способом).

д) Существует единственное линейное отображение s модуля $\Gamma^2(E)$ в $E \times E$ такое, что $s(\gamma(x)) = x \otimes x$ для всех $x \in E$; показать, что если модуль E свободный, то s является изоморфизмом на подмодуль симметрических тензоров порядка 2 на модуле E.

е) Пусть $A = \boldsymbol{Z}$, и E — циклическая группа конечного порядка n. Показать, что $\Gamma^2(E)$ — циклическая группа порядка n, если n нечетно, и порядка $2n$, если n четно. (Заметить прежде всего, что если a — образующий элемент группы E, то $\gamma(a)$ — образующий группы $\Gamma^2(E)$, и что для любого целого h $\gamma(-ha) = \gamma(ha)$; если n нечетно, то при $h = (n-1)/2$ вывести отсюда, что $n\gamma(a) = 0$; точно так же получить равенство $2n\gamma(a) = 0$ при n четном. Наконец, доказать, что если n нечетно (соответственно четно), то существует квадратическое отображение Q группы E в циклическую группу порядка n (соответственно $2n$), переводящее элемент a в образующий этой группы.)

8) Пусть A — поле, E, F — векторные пространства над полем A. Пусть g — отображение пространства E в F такое, что существуют три отображения a, b, c произведения $E \times E$ в F, удовлетворяющие равенству

$$g(\lambda x+\mu y)=\lambda^2 a(x, y)+\lambda\mu b(x, y)+\mu^2 c(x, y) \qquad (4)$$

для любых $x, y \in E$, $\lambda, \mu \in E$.

а) Доказать равенства: $a(x, y)=g(x)$, $c(x, y)=g(y)$, $b(y, x)=-b(x, y)$, $b(\lambda x, y)=\lambda b(x, y)$; показать, кроме того, что, положив

$$d(x, y, z)=b(x+y, z)-b(x, z)-b(y, z),$$

будем иметь равенства $d(x, y, z) = d(y, z, x) = d(z, x, y)$; вывести отсюда, что $d(\lambda x, \mu y, \nu z) = \lambda\mu\nu d(x, y, z)$.

б) Вывести из а), что если $A \neq \boldsymbol{F}_2$, то обязательно $d(x, y, z) = 0$ и, следовательно, отображение g — квадратическое (упражнение 7). Напротив, для $A = \boldsymbol{F}_2$ и $\dim E \geqslant 3$ доказать, что существуют отображения g пространства E в A, удовлетворяющие условию (4), для которых $d(x, y, z)$ — не тождественный нуль.

9) Пусть A — коммутативное кольцо, E — A-модуль, имеющий базис из n элементов, Φ — симметрическая билинейная форма на модуле E. Пусть e — элемент модуля $\bigwedge^n E$, образующий базис этого модуля, Δ — дискриминант формы Φ относительно e, φ_p — канонический изоморфизм модуля $\bigwedge^p E$ на $\bigwedge^{n-p} E^*$ относительно e (гл. III, § 8, n° 5). Положим $d_{(p)}(x) = \varphi_{n-p}^{-1}(d_{\Phi(p)}(x))$, $x \in \bigwedge^p E$; показать, что отображение $d_{(p)}$ модули $\bigwedge^p E$ в $\bigwedge^{n-p} E$ обладает следующими свойствами:

а) $d_{(n-p)}(d_{(p)}(x)) = (-1)^{p(n-p)}\Delta x$ для любого $x \in \bigwedge^p E$.

б) $x \wedge d_{(p)}(y) = \Phi_{(p)}(x, y)\, e$ и $\Phi_{(n-p)}(d_{(p)}(x), d_{(p)}(y)) = \Delta\Phi_{(p)}(x, y)$ для любых элементов $x, y \in \bigwedge^p E$.

в) Предположим дополнительно, что A — поле и форма Φ невырождена. Тогда, если x — разложимый p-вектор $\neq 0$, соответствующий подпространству F пространства E (гл. III, § 7, n° 3), то $d_{(p)}(x)$ — разложимый $(n-p)$-вектор $\neq 0$, соответствующий подпространству F^0, ортогональному к F.

г) Распространить предыдущие результаты на случай, когда Φ — ε-эрмитова форма, полуторалинейная относительно некоторого инволютивного автоморфизма кольца $J \neq 1$ (A предполагается коммутативным).

10) а) Пусть A — коммутативное кольцо, E — A-модуль с базисом из трех элементов, Φ — симметрическая билинейная форма на модуле A. Для всяких двух элементов $x, y \in E$ положим $x \overline{\wedge} y = d_{(2)}(x \wedge y)$ (обозначения из упражнения 9) и элемент $x \overline{\wedge} y$ назовем *векторным произведением* x и y (относительно формы Φ и базиса

е модуля $\overset{3}{\bigwedge} E$). Показать, что $(x, y) \to x \overline{\bigwedge} y$ — знакопеременное билинейное отображение произведения $E \times E$ в E и что вектор $x \overline{\bigwedge} y$ ортогонален к x и y.

б) Пусть α, β — обратимые элементы кольца A, B — алгебра кватернионов над A, соответствующая паре (α, β) (гл. II, § 7, n° 8), $1, u, v, w$ — канонический базис алгебры B над кольцом A; пусть E — подмодуль в B с базисом u, v, w. Показать, что если кватернионы x и y *принадлежат подмодулю* E, то

$$xy = \Phi(x, y) + x \overline{\bigwedge} y,$$

где Φ — симметрическая билинейная форма на модуле E такая, что ассоциированные с Φ линейные отображения биективны, а $x \overline{\bigwedge} y$ — векторное произведение элементов x и y относительно формы Φ и базиса $\alpha^{-1}\beta^{-1} u \bigwedge v \bigwedge w$ модуля $\overset{3}{\bigwedge} E$.

11) Пусть Φ — невырожденная ε-эрмитова полуторалинейная форма на конечномерном векторном пространстве E. Векторное подпространство M пространства E называется *слабо ортогональным* к подпространству N (относительно формы Φ), если одно из подпространств M и N^0 содержит другое.

а) Доказать, что отношение «M слабо ортогонально к N» симметрично.

б) Если подпространства M и N слабо ортогональны, то и M^0 и N^0 слабо ортогональны.

в) Если подпространства M и N слабо ортогональны и $M \cap N = \{0\}$, то M и N ортогональны.

§ 4. Вполне изотропные подпространства. Теорема Витта

В этом параграфе предполагается, что кольцо A, если не оговорено противное, является телом, Φ — либо ε-эрмитова форма на модуле E (относительно инволютивного антиавтоморфизма $\lambda \to \overline{\lambda}$ тела A), либо симметрическая билинейная форма, ассоциированная с квадратичной формой Q на модуле E (в последнем случае тело A предполагается коммутативным).

1. *Изотропные подпространства*

Определение 1. *Элемент x* модуля E *над* кольцом A *называется изотропным, если* $\Phi(x, x) = 0$. *Подмодуль F модуля E называется*

1) *изотропным, если существует ненулевой элемент $x \in F$, ортогональный к F;*

2) *вполне изотропным, если сужение формы* Φ *на подмодуль* F *равно нулю.*

Если на модуле E задана квадратичная форма Q, то элемент модуля E называется изотропным (соответственно подмодуль называется изотропным или вполне изотропным), если этот элемент изотропен (соответственно подмодуль изотропен или вполне изотропен) относительно билинейной формы, ассоциированной с Q.

Изотропный вектор — это вектор, ортогональный к самому себе. Подмодуль F изотропен в точности тогда, когда $F \cap F^0 \neq \{0\}$, то есть сужение формы Φ на F вырождено; таким образом, *неизотропный* подмодуль G модуля E — это такой подмодуль, сужение формы Φ на который не вырождено. Для того чтобы подмодуль F модуля E был вполне изотропным, необходимо и достаточно, чтобы $F \subset F^0$. Если F — вполне изотропный подмодуль, то любой подмодуль F', содержащийся в F, также изотропен. Сумма любого семейства попарно ортогональных вполне изотропных подмодулей является вполне изотропным подмодулем. Множество вполне изотропных подмодулей модуля E, упорядоченное по включению, очевидно, индуктивно; отсюда следует, что всякий вполне изотропный подмодуль содержится в некотором *максимальном* вполне изотропном подмодуле.

Предложение 1. *Пусть* A *— тело. Если неизотропное подпространство* F *пространства* E *конечномерно, то* E *является прямой суммой подпространств* F *и* F^0.

В самом деле, по предположению, сужение Φ' формы Φ на подпространство Φ не вырождено, и поэтому отображение $d_{\Phi'}$ подпространства F в сопряженное подпространство F^*, ассоциированное справа с формой Φ, инъективно, а значит, и биективно, поскольку подпространства F и F^* имеют одинаковую размерность. Следовательно, для каждого $y \in E$ существует единственный элемент $y_0 \in F$ такой, что $\Phi(x, y) = \Phi(x, y_0)$ для любого $x \in F$, то есть $y - y_0 \in F^0$; это и доказывает, что пространство E является прямой суммой F и F^0.

Следствие. *Если подпространство* F *пространства* E *конечномерно и форма* Φ *невырождена, то следующие условия эквивалентны:*

а) F *неизотропно*,

б) F^0 *неизотропно*,

в) E — *прямая сумма* F *и* F^0.

В самом деле, по предложению 1, из условия а) следует в), а из в) следуют условия а) и б). Наконец, если подпространство F^0 неизотропно, то $F \cap F^0 \subset F^0 \cap F^{00} = \{0\}$, так что F также неизотропно, то есть условие а) следует из б).

Определение 2. *Пусть* Q — *квадратичная форма на модуле* E. *Элемент* $x \in E$ *называется сингулярным* (*относительно формы* Q), *если* $Q(x) = 0$. *Подмодуль* F *модуля* E *называется*

1) *сингулярным, если существует ненулевой сингулярный элемент* $x \in F$, *ортогональный к* F;

2) *вполне сингулярным, если сужение формы* Q *на* F *равно нулю*.

Ядро квадратичного модуля (E, Q) (§ 3, n° 4) состоит из сингулярных элементов модуля E^0; для того чтобы подмодуль F был сингулярным, необходимо и достаточно, чтобы его ядро было отлично от $\{0\}$. Так как $\Phi(x, y) = Q(x + y) - Q(x) - Q(y)$, то всякий отличный от $\{0\}$ вполне сингулярный модуль сингулярен. Так как $\Phi(x, x) = 2Q(x)$, то всякий сингулярный вектор изотропен и всякий сингулярный (соответственно вполне сингулярный) подмодуль изотропен (соответственно вполне изотропен). Обратное верно, если A — тело характеристики $\neq 2$. Всякий подмодуль, содержащийся во вполне сингулярном подмодуле, вполне сингулярен. Сумма любого семейства попарно ортогональных вполне сингулярных подмодулей будет вполне сингулярным подмодулем. Множество вполне сингулярных подмодулей модуля E, упорядоченное по включению, индуктивно; поэтому всякий вполне сингулярный подмодуль содержится в *максимальном* вполне сингулярном подмодуле.

2. *Разложение Витта*

К условиям, уже наложенным в начале этого параграфа, мы добавим следующее:

Условие (Т). *Для всякого* $x \in E$ *существует элемент* $\alpha \in A$ *такой, что* $\Phi(x, x) = \alpha + \varepsilon\bar{\alpha}$.

Это условие всегда выполнено, если форма Φ знакопеременная или если $\varepsilon = 1$ и A — тело характеристики $\neq 2$, когда можно взять $\alpha = \frac{1}{2}\Phi(x, x)$ (см. упражнения 1 и 14).

Лемма 1. *Пусть* Φ — *ε-эрмитова форма, удовлетворяющая условию* (T) (соответственно *билинейная форма, ассоциированная с квадратичной формой* Q) *на пространстве* E, *и* F — *вполне изотропное* (соответственно *вполне сингулярное*) *подпространство пространства* E, *отличное от нуля. Для всякого элемента* $x \in E$, *не ортогонального к* F, *и всякого* $\alpha \in A$ *существует такой элемент* $y \in F$, *что* $\Phi(x + y, x + y) = \alpha + \varepsilon\bar{\alpha}$ (соответственно $Q(x+y) = \alpha$).

В самом деле, положим $\Phi(x, x) = \beta + \varepsilon\bar{\beta}$ (соответственно $Q(x) = \beta$). Если $y \in F$, то $\Phi(x + y, x + y) = (\beta + \Phi(x, y)) + \varepsilon\overline{(\beta + \Phi(x, y))}$, так как $\Phi(y, y) = 0$ (соответственно $Q(x + y) = \beta + \Phi(x, y)$, так как $Q(y) = 0$). Поскольку x не ортогонален к F, аффинная линейная функция $y \to \Phi(x, y) + \beta$ на подпространстве F не равна константе. Следовательно, она принимает значение α для некоторого элемента $y \in F$. Этот элемент и есть искомый.

Разложением Витта модуля E называется всякое его разложение в прямую сумму трех подпространств F, F' и G таких, что F и F' вполне изотропны (соответственно вполне сингулярны), а G неизотропно и ортогонально к сумме $F + F'$; если пространство E конечномерно, то матрица формы Φ относительно некоторого базиса, подобранного подходящим образом для разложения Витта, имеет вид

$$\begin{pmatrix} 0 & U & 0 \\ \varepsilon\bar{U} & 0 & 0 \\ 0 & 0 & V \end{pmatrix}. \tag{1}$$

Форма Φ называется *нейтральной*, если она невырождена, а пространство E конечномерно и разлагается в прямую сумму двух вполне изотропных (соответственно вполне сингулярных) подпространств. Прямая сумма двух нейтральных форм является нейтральной формой.

Предложение 2. *Пусть* Φ — *невырожденная* ε-*эрмитова форма, удовлетворяющая условию* (T) (соответственно *билинейная форма, ассоциированная с невырожденной квадратичной формой* Q), *и* F — *вполне изотропное* (соответственно *вполне сингулярное*) *подпространство конечной размерности* r.

а) *Если вполне изотропное подпространство* F' *размерности* r *удовлетворяет условию* $F' \cap F^0 = \{0\}$, *то сумма* $F + F'$ *неизотропна и для всякого базиса* (f_i) *подпространства* F *существует базис* (f'_i) *подпространства* F' *такой, что* $\Phi(f_i, f'_j) = \delta_{ij}$ (*символ Кронекера*) *для* $i, j = 1, \ldots, r$.

б) *Если вполне изотропное* (соответственно *вполне сингулярное*) *подпространство* G *размерности* $\leqslant r$ *удовлетворяет условию* $G \cap F^0 = \{0\}$, *то существует вполне изотропное* (соответственно *вполне сингулярное*) *подпространство* $F' \supset G$ *размерности* r *и такое, что* $F' \cap F^0 = \{0\}$.

Пусть Ψ — сужение формы Φ на произведение $F \times F'$; если $x' \in F'$, то из утверждения $\Phi(x, x') = 0$ для любого $x \in F$ следует, что $x = 0$, поскольку $F' \cap F^0 = \{0\}$. Поэтому вторая часть утверждения а), кроме неизотропности подпространства $F + F'$, получается из следствия к предложению 1 § 1, n° 6.

Далее, подпространство $H = (F + F') \cap (F + F')^0$ равно $(F + F') \cap F^0 \cap F'^0$. Так как $F \subset F^0$, то $(F + F') \cap F^0 = F + (F' \cap F^0) = F$, откуда $H = F \cap F'^0$; поскольку форма Ψ невырождена, то $H = \{0\}$. Это и означает, что сумма $F + F'$ неизотропна.

Для доказательства утверждения б) проведем индукцию по числу $s = \dim G$. Достаточно доказать, что для $s < r$ существует вполне изотропное (соответственно вполне сингулярное) подпространство G' размерности $s+1$, содержащее G и такое, что $G' \cap F^0 = \{0\}$. Так как $\dim G < \dim F$, сужение формы Φ на произведение $F \times G$ вырождено, и $F \cap G^0 \neq \{0\}$, поскольку $G \cap F^0 = \{0\}$. В подпространстве G^0 существует элемент x, не входящий в сумму $G + F^0$; если бы выполнялось включение $G + F^0 \supset G^0$, то, перейдя к ортогональным подпространствам и заметив, что $F = F^{00}$ и $G = G^{00}$ (§ 1, n° 6, следствие 1 предложения 4), мы получили бы включение $G^0 \cap F \subset G$, откуда

$$G^0 \cap F \subset G \cap F \subset G \cap F^0 = \{0\},$$

что неверно. Так как $F \subset F^0$, то, прибавив к элементу $x \in G^0$ некоторый вектор из пересечения $G^0 \cap F$, мы не изменим его свойств. Поскольку подпространство $G^0 \cap F$ вполне изотропно (соответственно вполне сингулярно) и отлично от $\{0\}$, то в силу леммы 1 элемент x можно выбрать изотропным (соответственно сингулярным). Тогда подпространство $G' = G + Ax$ имеет размерность $s + 1$ и вполне изотропно (соответственно вполне сингулярно); более того, $G' \cap F^0 = \{0\}$: если элемент $y = z + ax$ ($z \in G$, $a \in A$) входит в F^0, то $a = 0$, ибо в противоположном случае $x \in F^0 + G$, что противоречит выбору элемента x; поэтому $y = z \in G \cap F^0 = \{0\}$, то есть $y = 0$. Следовательно, G' — искомое подпространство.

Следствие 1. *Для всякого вполне изотропного* (соответственно *вполне сингулярного*) *подпространства F размерности r существует вполне изотропное* (соответственно *вполне сингулярное*) *подпространство F' размерности r такое, что $F \cap F' = \{0\}$ и подпространство $F + F'$ неизотропно.*

Для доказательства достаточно в предложении 2б) положить $G = \{0\}$.

Следствие 2. *Любые две нейтральные ε-эрмитовы формы на пространствах одинаковой размерности эквивалентны.*

Замечание. В условиях следствия 1 пространство E является прямой суммой подпространства $F + F'$ и ортогонального к нему подпространства. Следовательно, это разложение Витта для пространства E. В силу предложения 2а) в подпространствах F и F' можно выбрать такие базисы, что блок U в матрице (1) формы Φ будет единичной матрицей 1_r.

Предложение 3. *Пусть Φ — невырожденная ε-эрмитова форма, удовлетворяющая условию* (T) (соответственно *билинейная форма, ассоциированная с невырожденной квадратичной формой Q*). *Пусть, далее F_1 и F_2 — максимальные вполне изотропные* (соответственно *вполне сингулярные*) *подпространства пространства E, одно из которых имеет конечную размерность. Положим $F = F_1 \cap F_2$. Пусть S_i ($i = 1, 2$) — дополнение подпространства F в F_i; положим $S = S_1 + S_2$. Тогда существуют подпространства G и H пространства E такие, что*

а) *подпространства* $G + F$, S *и* H *неизотропны и попарно ортогональны*;

б) E *есть прямая сумма подпространств* F, S, G, H;

в) *в* H *не существует ненулевых изотропных* (соответственно *сингулярных*) *векторов*;

г) G *вполне изотропно* (соответственно *вполне сингулярно*). *Более того, оба подпространства* F_1 *и* F_2 *конечномерны и* $\dim F_1 = \dim F_2$, $\dim G = \dim F$, $\dim S_1 = \dim S_2$, $\operatorname{codim} H = 2 \dim F_1$.

Заметим прежде всего, что если N — максимальное вполне изотропное (соответственно вполне сингулярное) подпространство, то всякий изотропный (соответственно сингулярный) вектор x, ортогональный к N, входит в x, ибо в противоположном случае существование подпространства $N + Ax$ противоречило бы максимальности N. Таким образом, если $x_i \in F_i^0$ $(i = 1, 2)$ — изотропный (соответственно сингулярный) вектор, то $x_i \in F_i$. С другой стороны, если элемент $y \in S_1$ ортогонален к S_2, то он ортогонален и к F_1, поскольку F_1 вполне изотропно, а следовательно, и к F, то есть ортогонален к $F_2 = S_2 + F$. Так как элемент y изотропен (соответственно сингулярен), то

$$y \in S_1 \cap S_2 = S_1 \cap F_1 \cap F_2 = S_1 \cap F = \{0\}.$$

Следовательно, $S_1 \cap S_2^0 = \{0\}$ и аналогично $S_2 \cap S_1^0 = \{0\}$.

Так как одно из подпространств F_1 и F_2, скажем F_1, конечномерно, то S_1 конечномерно, и следовательно, S_1^0 имеет конечную коразмерность (§ 1, п° 6, следствие 1 предложения 4). Поэтому S_2 конечномерно, так как $S_2 \cap S_1^0 = \{0\}$; более того, отсюда следует соотношение $\dim S_2 \leqslant \operatorname{codim} S_1^0 = \dim S_1$; аналогично $\dim S_1 \leqslant \dim S_2$, так что $\dim S_1 = \dim S_2$. В силу предложения 2а) подпространство $S = S_1 + S_2$ неизотропно.

Тогда подпространство N, ортогональное к S, неизотропно (п° 1, следствие предложения 1) и содержит F. Тем самым, по следствию 1 предложения 2, существует вполне изотропное (соответственно вполне сингулярное) подпространство G пространства N такое, что $\dim G = \dim F$, $G \cap F = \{0\}$, и подпространство $G + F$ неизотропно. Таким образом, утверждение г) установлено. Взяв в качестве H подпространство в N, ортогональное к $G + F$, мы установим справедливость а) и б). Далее, ввиду замечания в начале доказательства и равенства $H \cap F_1 = \{0\}$,

подпространство H, ортогональное к $F_1 = S_1 + F$, не может содержать ненулевых изотропных (соответственно сингулярных) векторов. Это доказывает утверждение в). Наконец, некоторые из равенств, относящихся к размерностям, установлены в ходе доказательства, а остальные тривиально следуют из них.

Следствие 1. *В предположениях предложения* 3, *любые два конечномерных максимальных вполне изотропных* (соответственно *вполне сингулярных*) *подпространства имеют одинаковую размерность. Для всякого конечномерного максимального вполне изотропного* (соответственно *вполне сингулярного*) *подпространства F существует другое подпространство F' с такими же свойствами, такое, что $F \cap F' = \{0\}$ и пространство $F + F'$ неизотропно.*

Если $F \cap F' = \{0\}$, то, в обозначениях предложения 3, $G = \{0\}$ и $F + F'$ неизотропно. Остальные утверждения тривиально следуют из предложения 3 и следствия 1 предложения 2.

Следствие 2. *Пусть Q — невырожденная квадратичная форма на векторном пространстве E конечной размерности n над алгебраически замкнутым полем A. Тогда в E существует базис $(e_i)_{1 \leqslant i \leqslant n}$ такой, что*

$$Q\left(\sum_{i=1}^{n} x_i e_i\right) = \sum_{i=1}^{\nu} x_i x_{i+\nu}, \qquad \text{если } n = 2\nu, \tag{2}$$

$$Q\left(\sum_{i=1}^{n} x_i e_i\right) = \sum_{i=1}^{\nu} x_i x_{i+\nu} + x_{2\nu+1}^2, \text{ если } n = 2\nu + 1. \tag{3}$$

В самом деле, пусть F_1 и F_2 — максимальные вполне сингулярные подпространства, $F_1 \cap F_2 = \{0\}$ и q — их размерность. Тогда, в обозначениях предложения 3, $G = \{0\}$. Взяв в F_1 и F_2 такие базисы $(e_i)_{1 \leqslant i \leqslant q}$ и $(e_i)_{q+1 \leqslant i \leqslant 2q}$, что $\Phi(e_i, e_{j+q}) = \delta_{ij}$ для $i, j = 1, \ldots, q$ (предложение 2а)), получим, что достаточно доказать неравенство $\dim H \leqslant 1$. Но если $x \in H$, $y \in H$ и $x \neq 0$, то уравнение

$$Q(y - ax) = Q(y) - a\Phi(x, y) + a^2 Q(x) = 0$$

имеет по крайней мере одно решение a_0 (поскольку $Q(x) \neq 0$), и тогда $y = a_0 x$, так как единственный сингулярный вектор H — нулевой.

Определение 3. *Пусть пространство E конечномерно и* Ф — *невырожденная ε-эрмитова форма, удовлетворяющая условию* (T) (соответственно *билинейная форма, ассоциированная с невырожденной квадратичной формой Q*). *Индексом формы* Ф (соответственно *формы Q*) *называется общая размерность максимальных вполне изотропных* (соответственно *вполне сингулярных*) *подпространств пространства E.*

Если размерность E равна n, а индекс формы Ф (соответственно *формы Q*) *равен ν, то из предложения* 3 *следует неравенство*

$$n \geqslant 2\nu. \tag{4}$$

Более того, поскольку всякое вполне изотропное (соответственно вполне сингулярное) подпространство содержится в максимальном вполне изотропном (соответственно вполне сингулярном) подпространстве, то максимальными вполне изотропными (соответственно вполне сингулярными) подпространствами будут в точности те, размерность которых равна ν.

Утверждение, что форма Ф (соответственно Q) имеет индекс 0, означает, что E не имеет ненулевых изотропных (соответственно сингулярных) векторов. На пространстве четной размерности n нейтральными будут формы индекса $\frac{1}{2}n$; на пространстве нечетной размерности нейтральных форм не существует. Предложение 3 показывает, что всякая форма является прямой суммой нейтральной формы и формы индекса 0.

Предложение 4. *Пусть Q — невырожденная квадратичная форма на пространстве E, и существует ненулевой вектор $x \in E$ такой, что $Q(x) = 0$. Тогда для всякого элемента $a \in A$ существует $y \in E$ такой, что $Q(y) = a$.*

В самом деле, по следствию 1 предложения 2, существует подпространство $G = F + F'$ (F и F' — вполне сингулярные подпространства размерности 1) пространства E размерности 2, такое, что сужение формы Q на G — нейтральная форма.

Пусть $\{e, e'\}$ ($e \in F$, $e' \in F'$) — некоторый базис подпространства G; тогда имеем

$$Q(xe + x'e') = bxx' \qquad (x \in A,\ x' \in A,\ b \in A,\ b \neq 0).$$

Таким образом, достаточно взять $y = ae + b^{-1}e'$.

3. Теорема Витта

Пусть E и E' — векторные пространства над телом A, Φ и Φ' (соответственно Q и Q')— полуторалинейные (соответственно квадратичные) формы на E и E'. Метрическим гомоморфизмом пространства E в E' называется всякое линейное отображение u пространства E в E', удовлетворяющее условию $\Phi'(u(x), u(y)) = \Phi(x, y)$ (соответственно $Q'(u(x)) = Q(x)$) для любых $x \in E$, $y \in E$. Если E и E' имеют одинаковую конечную размерность и форма Φ (соответственно форма Q) невырождена, то всякий метрический гомоморфизм u пространства E в E' будет изоморфизмом, так как равенство $u(x) = 0$ влечет за собой, что $\Phi(x, y) = 0$ для любого $y \in E$, то есть $x = 0$; поэтому гомоморфизм u инъективен, а следовательно, и биективен, поскольку E и E' имеют одну и ту же конечную размерность.

Теорема 1 (Витт). *Пусть E и E' — конечномерные векторные пространства, наделенные соответственно невырожденными ε-эрмитовыми формами Φ и Φ', удовлетворяющими условию* (T) n° 2 (соответственно *невырожденными квадратичными формами Q и Q'*), *и эти структуры изоморфны. Тогда всякий инъективный метрический гомоморфизм некоторого подпространства F пространства E в E' можно продолжить до метрического изоморфизма пространства E на E'.*

Поскольку структуры E и E' изоморфны, достаточно показать, что всякий инъективный метрический гомоморфизм подпространства F в E можно продолжить до метрического автоморфизма пространства E. Заметим, что если F_i $(i = 1, 2)$— подпространство в E, $F_1 \cap F_2 = \{0\}$ и u_i — метрический гомоморфизм подпространства F_i в E такой, что $\Phi(u_1(x_1), u_2(x_2)) = \Phi(x_1, x_2)$ для $x_i \in F_i$ $(i = 1, 2)$, то гомоморфизм v: $x_1 + x_2 \to u_1(x_1) + u_2(x_2)$ суммы $F_1 + F_2$ в E, являющийся продолжением гомоморфизмов u_1 и u_2, также метрический: в самом деле, разложение каждого из выражений $\Phi(x_1 + x_2, y_1 + y_2)$ и $\Phi(u_1(x_1) + u_2(x_2), u_1(y_1) + u_2(y_2))$ (соответственно $Q(x_1 + x_2)$ и $Q(u_1(x_1) + u_2(x_2))$) содержит четыре (соответственно три) члена, и при сделанных предположениях эти члены соответственно равны. Кроме того, если гомоморфизмы u_1 и u_2 инъек-

тивны и $u_1(F_1) \cap u_2(F_2) = \{0\}$, то гомоморфизм v также инъективен.

1) Докажем теорему Витта прежде всего *в случае, когда множество точек, инвариантных относительно гомоморфизма u, образует гиперплоскость U пространства F.* Тогда множество векторов вида $u(x) - x$, где $x \in F$, будет некоторой прямой D.

Если подпространство F' ортогонально к D и $F' \cap F = F' \cap u(F) = 0$, то для всех $x \in F$, $y \in F'$ выполняется равенство $\Phi(u(x), y) = \Phi(x, y)$. Применив к гомоморфизму u и тождественному отображению F' в E замечание, сделанное в начале доказательства, получим, что гомоморфизм u продолжается на $F + F'$, причем точки подпространства F' остаются фиксированными; множество векторов вида $u(x) - x$ $(x \in F + F')$ есть та же прямая D. Но для $x \in F$, $y \in F$ имеем

$$\Phi(u(x), u(y) - y) = \Phi(u(x), u(y)) - \Phi(u(x), y) = \Phi(x - u(x), y), \tag{5}$$

откуда при $x \in U$ (то есть $u(x) = x$) следует, что $x \in D^0$; другими словами, $U \subset D^0$. Будем различать два случая:

а) $F \not\subset D^0$. Формула (5) показывает, что $u(F)$ не содержится в D^0, так что $F \cap D^0 = u(F) \cap D^0 = U$. В качестве F' возьмем дополнение подпространства U в D^0; так как $F + F'$ содержит гиперплоскость U и отлична от нее, то $F + F' = E$, так что в этом случае искомое продолжение гомоморфизма u на E найдено.

б) $F \subset D^0$. Тогда по формуле (5) $u(F) \subset D^0$, следовательно, $D \subset D^0$, то есть прямая D изотропна (соответственно сингулярна, так как для $x \in F$ выполняются равенства $Q(u(x) - x) = Q(u(x)) - \Phi(x, u(x)) + Q(x) = 2Q(x) - \Phi(x, x) = 0$). Покажем, что при этих условиях в D^0 существует подпространство F', являющееся дополнением подпространств F и $u(F)$ в D^0. Это ясно, если $F = u(F)$. Если же это неверно, то возьмем такие векторы x и y, что $x \in F$, $x \overline{\in} U$, $y \in U(F)$, $y \overline{\in} U$; тогда $F = U + Ax$, $u(F) = U + Ay$ и F не содержит суммы $x + y$: иначе элемент $y = (x + y) - x$ принадлежал бы к $F \cap u(F) = U$; аналогично сумма $x + y$ не входит в $u(F)$; таким образом, прямая $A(x + y)$ является дополнением подпространств F и $u(F)$ в подпространстве $F + u(F)$; теперь достаточно положить $F' = A(x + y) + G$, где G — дополнение подпространства $F + u(F)$ в D^0. Тогда будут

выполнены равенства $F + F' = u(F) + F' = D^0$ и рассуждение, проведенное в начале 1), показывает, что и в данном случае существует продолжение гомоморфизма u на гиперплоскость D^0 пространства E, причем D^0 устойчива относительно этого продолжения.

Следовательно, остается рассмотреть случай, когда F есть гиперплоскость D^0 и u — автоморфизм подпространства F. Докажем, что для любого $z \in E$ существует вектор $z' \in E$ такой, что

$$\Phi(u(x), z') = \Phi(x, z) \tag{6}$$

для любого $x \in F$; в самом деле, линейная форма $x \to \Phi(u^{-1}(x), z)$ на F является сужением некоторой линейной формы на E, именно формы типа $x \to \Phi(x, z')$, так как форма Φ невырождена; следовательно, равенство (6) верно; более того, если $z \in F$, то существует вектор $z' \in E$, удовлетворяющий условию (6) и такой, что $\Phi(z', z') = \Phi(z, z)$ (соответственно $Q(z) = z$): в самом деле, поскольку $F = D^0$, равенство (6) сохраняется, если к вектору z прибавить любой элемент $u(y) - y$ ($y \in F$) прямой D; так как вектор z не ортогонален к D, то доказываемое утверждение следует из леммы 1 n° 2. Замечание, сделанное в начале доказательства, показывает, что существует метрический гомоморфизм v пространства $F + Az = E$ в E, являющийся продолжением гомоморфизма u и переводящий вектор z в z'. Поскольку форма Φ не вырождена, v — искомый метрический автоморфизм пространства E.

2) В общем случае проведем индукцию по числу $r = \dim F$. Случай $r = 0$ тривиален. Пусть $r > 0$, то есть $F \neq \{0\}$, и пусть U — гиперплоскость в F. Сужение u_0 гомоморфизма u на U, по предположению индукции, может быть продолжено до метрического автоморфизма v_0 пространства E. Если v_0 является продолжением гомоморфизма u, то теорема доказана. Если же это не так, то U является множеством элементов, инвариантных относительно $v_0^{-1}u$, и, по случаю 1), существует метрический автоморфизм v_1 пространства E, являющийся продолжением гомоморфизма $v_0^{-1}u$. Тогда автоморфизм $v_0 v_1$ будет искомым продолжением гомоморфизма u, что и требовалось доказать.

Следствие 1. *Пусть* E_i ($i = 1, 2$)— *конечномерные векторные пространства,* Φ_i — *невырожденная* ε-*эрмитова форма на* E_i,

удовлетворяющая условию (T) (соответственно Q_i — *невырожденная квадратичная форма на* E_i). *Пусть, далее,* E_i *является прямой суммой своих ортогональных подпространств* E_i' *и* E_i''. *Если формы* Φ_1 *и* Φ_2 (соответственно Q_1 *и* Q_2) *эквивалентны и их сужения на* E_1' *и* E_2' *эквивалентны, то их сужения на* E_1'' *и* E_2'' *также эквивалентны.*

В самом деле, пусть u — метрический изоморфизм подпространства E_1' на E_2'. По теореме 1 его можно продолжить до метрического изоморфизма v пространства E_1 на E_2. Так как форма Φ_i невырождена и E_i'' ортогонально к E_i' в E_i, то изоморфизм v отображает E_1'' на E_2'', что и требовалось доказать.

Следствие 2. *В предположениях теоремы* 1 *группа метрических автоморфизмов пространства* E *транзитивно переставляет его вполне изотропные* (соответственно *вполне сингулярные*) *подпространства данной размерности. Более того, всякое биективное линейное отображение вполне изотропного* (соответственно *вполне сингулярного*) *подпространства* F *пространства* E *на* F *индуцируется некоторым метрическим автоморфизмом пространства* E.

Следствие 3. *Пусть* Q — *невырожденная квадратичная форма на конечномерном векторном пространстве над алгебраически замкнутым полем* A. *Группа метрических автоморфизмов пространства* E *транзитивно переставляет его неизотропные подпространства данной размерности.*

Это сразу же вытекает из теоремы 1 и следствия 2 предложения 3.

Упражнения. 1) а) Пусть K — тело характеристики 2, $J : \xi \to \overline{\xi}$ — инволютивный антиавтоморфизм тела K, Z — центр тела K. Показать, что если сужение антиавтоморфизма J на Z не тождественно, то всякий элемент $\mu \in K$ такой, что $\overline{\mu} = \mu$, имеет вид $\lambda + \overline{\lambda}$ (заметить, что в Z содержится элемент $\varrho \neq 0$, который может быть записан в виде $\zeta + \overline{\zeta}$, где $\zeta \in Z$); в этом случае всякая эрмитова форма на векторном пространстве над телом K удовлетворяет условию (T).

б) Привести пример тела характеристики 2, обладающего инволютивным антиавторфизмом $\xi \to \overline{\xi}$, отличным от тождественного, и в котором существуют элементы $\mu = \overline{\mu}$, не имеющие вида $\lambda + \overline{\lambda}$ (см. гл. VIII, § 11, упражнение 4).

2) Пусть A — тело, E — векторное пространство над A, Φ — невырожденная ε-эрмитова форма на E, удовлетворяющая условию (T) (соответственно Q — невырожденная квадратичная форма на E, Φ — симметрическая билинейная форма, ассоциированная с формой Q).

а) Доказать, что плоскость $P \subset E$ изотропна (соответственно сингулярна), но не вполне изотропна (соответственно не вполне сингулярна) тогда и только тогда, когда она не содержит ни одной изотропной (соответственно сингулярной) прямой (см. упражнение 14д)).

б) Предположим, что $\dim E \geqslant 3$ и что в E существуют ненулевые изотропные векторы. Показать, что для всякой не вполне изотропной плоскости P в пространстве E существует неизотропное векторное подпространство $V \subset E$ размерности 3, содержащее ненулевые изотропные векторы и такое, что $P \subset V$.

3) Показать, что в предположениях упражнения 2 и при условии $\dim E \geqslant 3$ всякая изотропная прямая в пространстве E является пересечением двух неизотропных плоскостей.

4) Сохраняя предположения упражнения 2, будем считать дополнительно, что пространство E конечномерно.

а) Показать, что если индекс ν формы Φ (соответственно Q) $\geqslant 1$, то для всякого ненулевого изотропного (соответственно сингулярного) вектора $a \neq 0$ существует базис (e_i) пространства E, составленный из изотропных (соответственно сингулярных) векторов и такой, что $e_1 = a$ (см. упражнение 14д)).

б) Пусть V, W — вполне изотропные (соответственно вполне сингулярные) подпространства одинаковой размерности $r \leqslant \nu$; показать, что существуют максимальные вполне изотропные (соответственно вполне сингулярные) подпространства V_1, W_1 такие, что $V \subset V_1$, $W \subset W_1$ и $V_1 \cap W_1 = V \cap W$. (Если $U = V \cap W$, проводить рассуждения в факторпространстве U^0/U.)

в) Пусть V, W, V_1, W_1 — вполне изотропные (соответственно вполне сингулярные) подпространства одинаковой размерности, и подпространства $V + W$ и $V_1 + W_1$ неизотропны. Показать, что существует метрический автоморфизм u пространства E такой, что $u(V) = V_1$ и $u(W) = W_1$.

г) Пусть f — линейная форма на пространстве E, и α — элемент тела A, имеющий вид $\lambda + \varepsilon\bar{\lambda}$ (соответственно элемент тела A). Рассмотрим на E полуторалинейную форму

$$(x, y) \longrightarrow \Phi_1(x, y) = \Phi(x, y) + f(x)\,\alpha\overline{f(y)}$$

(соответственно квадратичную форму

$$x \longrightarrow Q_1(x) = Q(x) + \alpha(f(x))^2).$$

Показать, что если форма Φ_1 (соответственно Q_1) невырождена и ее индекс равен ν_1, то $|\nu_1 - \nu| \leqslant 1$.

5) а) Пусть B — кольцо, $\xi \to \overline{\xi}$ — его инволютивный антиавтоморфизм, ε — элемент центра кольца B такой, что $\varepsilon\overline{\varepsilon} = 1$. Показать, что для любого обратимого элемента β кольца K, удовлетворяющего условию $\beta + \varepsilon\overline{\beta} \neq 0$, существует обратимый элемент $\mu \neq 1$ такой, что $\mu(\beta + \varepsilon\overline{\beta})\mu = \beta + \varepsilon\overline{\beta}$. (Показать, что можно взять такой элемент μ, для которого $\mu\beta\overline{\mu} = \beta$.)

б) Пусть A — тело, E — векторное пространство над A, Φ — невырожденная полуторалинейная ε-эрмитова форма на пространстве E, удовлетворяющая условию (Т). Показать, что если форма Φ не знакопеременная, то для любой неизотропной гиперплоскости H пространства E существует отличный от тождественного метрический автоморфизм пространства E, оставляющий неподвижным всякий элемент из H (использовать а)).

6) В предположениях упражнения 2 возьмем ненулевой изотропный вектор $a \in E$ (соответственно изотропный, но не сингулярный (заметим, что такие векторы существуют только в случае, когда характеристика тела A равна 2)). Пусть элемент $\lambda \in A$ обладает свойством $\lambda + \varepsilon\overline{\lambda} = 0$ (соответственно $\lambda = (Q(a))^{-1}$); показать, что сдвиг $x \to x + \Phi(x, a)\lambda a$ (гл. II, § 6, упражнение 7) является метрическим автоморфизмом пространства E; доказать обратное.

7) В предположениях упражнения 2 рассмотрим группу G метрических автоморфизмов пространства E. Показать, что единственными полулинейными биекциями пространства E на себя, перестановочными со всеми элементами группы G, являются гомотетии. Исключение представляют лишь три случая: $\dim E = 2$, G — группа метрических автоморфизмов, соответствующих квадратичной форме индекса 1 на пространстве E, и A — одно из трех тел: F_2, F_3 или F_4. (Воспользоваться упражнениями 5, 6 и 3; отдельно рассмотреть случай квадратичной формы на векторном пространстве размерности 2.)

°8) Пусть A — тело, E — векторное пространство конечной размерности > 0 над телом A, Φ — невырожденная полуторалинейная ε-эрмитова форма на пространстве E, удовлетворяющая условию (Т). Пусть $M(\Phi)$ — группа коэффициентов подобия пространства E относительно Φ (§ 6, n° 5).

а) Пусть V_1, V_2 — векторные подпространства в E, имеющие одинаковую размерность, и Φ_1, Φ_2 — сужения формы Φ на V_1, V_2 соответственно. Для того чтобы существовало подобие u такое, что $u(V_1) = V_2$, необходимо и достаточно, чтобы существовал такой элемент $\alpha \in M(\Phi)$, что формы $\alpha\Phi_1$ и Φ_2 эквивалентны (воспользоваться теоремой Витта).

б) Пусть (F, F', G) — разложение Витта пространства E (n° 2) и Φ_0 — сужение формы Φ на неизотропное подпространство G. Показать, что если $G \neq \{0\}$, то $M(\Phi) = M(\Phi_0)$. (Воспользоваться теоремой Витта и предложением 2 n° 2.)

в) Показать, что если индекс формы Φ равен ν и $\dim E = 2\nu$, то группа $M(\Phi)$ состоит из ненулевых элементов $\zeta \neq 0$ центра кольца A, удовлетворяющих условию $\bar{\zeta} = \zeta$. Если $\dim E = 2\nu + 1$, то группа $M(\Phi)$ состоит из элементов вида $\varrho\bar{\varrho}$, где $\varrho \neq 0$ пробегает мультипликативную группу ненулевых элементов центра кольца A (воспользоваться теоремой Витта). (См. § 10, упражнение 18.)

°9) Пусть A — поле, E — векторное пространство над полем A, Q — невырожденная квадратичная форма на E. *Подобием* относительно Q называется всякий автоморфизм u пространства E, для которого существует элемент $\alpha \in A$, отличный от нуля, такой, что $Q(u(x)) = \alpha Q(x)$ при любых $x \in E$; при этом автоморфизм u является также подобием относительно билинейной формы, ассоциированной с Q. Предполагая, что пространство E конечномерно, сформулировать и доказать результаты, аналогичные результатам из упражнения 8, для подобий относительно формы Q.

°10) Пусть A — тело, E — векторное пространство над телом A размерности $\geqslant 2$, Φ_1 (соответственно Φ_2) — невырожденная ε_1-эрмитова (соответственно ε_2-эрмитова) форма, полуторалинейная относительно антиавтоморфизма J_1 (соответственно J_2) тела A, удовлетворяющая условию (Т). Показать, что если группа метрических автоморфизмов пространства E относительно Φ_1 является подгруппой группы подобий относительно Φ_2, то существует элемент $\alpha \in A$ такой, что $\Phi_2 = \Phi_1\alpha$ (воспользоваться упражнениями 5б) и 6).

Доказать аналогичное свойство в случае, когда тело A коммутативно и вместо форм Φ_1 и Φ_2 в формулировке стоят невырожденные квадратичные формы Q_1, Q_2 на пространстве E.

11) Пусть A — кольцо, J — инволютивный антиавтоморфизм кольца A, E — A-модуль с конечным базисом (e_i), Φ — невырожденная ε-эрмитова форма на модуле E, R — матрица формы Φ относительно базиса (e_i); группа метрических автоморфизмов относительно Φ отождествляется с группой G обратимых матриц U таких, что ${}^tURU^J = R$.

а) Предположим, что существует матрица P такая, что $R = {}^tP + \varepsilon P^J$. Доказать, что для всякой матрицы S такой, что ${}^tS + \varepsilon S^J = 0$ и $P + S$ обратима, матрица $U = ({}^tP^J - \varepsilon^J S)^{-1}(P + S)$ входит в G, а матрица $\varepsilon I + U$ обратима. Доказать обратное (показать, что для всякой матрицы $U \in G$ такой, что $\varepsilon I + U$ обратима, выполняется равенство

$$\varepsilon(\varepsilon I + {}^tU)^{-1} R + \varepsilon^J R(\varepsilon^J I + U^J)^{-1} = R).$$

б) Показать, что условие утверждения а) выполняется, если форма Φ удовлетворяет условию (Т). В этом случае уравнение $2\xi = \alpha$ в кольце A имеет единственное решение при любом $\alpha \in A$.

*12) Пусть A — поле, E — векторное пространство над полем A конечной размерности n, Φ — невырожденная ε-эрмитова полуторалинейная форма на E.

а) Пусть u — эндоморфизм пространства E; показать, что если r_i $(1 \leqslant i \leqslant n)$ — инварианты подобия эндоморфизма u (гл. VII, § 5, n° 1, определение 1), то инвариантами подобия сопряженного относительно Ф эндоморфизма u^* являются многочлены $\overline{r}_i$ $(1 \leqslant i \leqslant m)$, где всякий $\overline{r}_i$ при применении к каждому коэффициенту автоморфизма J сводится к r_i (см. гл. VII, § 5, упражнение 2). Для любого неприводимого унитарного многочлена $p \in A[X]$, делящего минимальный многочлен эндоморфизма u, обозначим через $F_k(u, p)$ ядро эндоморфизма $(p(u))^k$ пространства E и через $F(u, p)$ — объединение ядер $F_k(u, p)$ для всех целых чисел $k > 0$. Показать, что если p и q — различные неприводимые унитарные многочлены, делящие минимальный многочлен эндоморфизма u, то подпространства $F(u, p)$ и $F(u^*, \overline{q})$ ортогональны (применить тождество Безу). Наконец, если подпространство G в E обладает свойством $u(G) \subset G$, то $u^*(G^0) \subset G^0$.

б) Предположим, что $uu^* = u^*u$ (в этом случае говорят, что эндоморфизм u нормален относительно Ф; см. § 7, n° 3); показать, что в этом случае $u^*(F_k(u, p)) \subset F_k(u, p)$ для любого k и, следовательно, $u^*(F(u, p)) \subset F(u, p)$. Положив $G(p, \overline{q}) = F(u, p) \cap \bigcap F(u^*, \overline{q})$, показать, что пространство E является прямой суммой подпространств $G(p, \overline{q})$ и что при $p \neq q_1$ и $p_1 \neq q$ подпространства $G(p, \overline{q})$ и $G(p_1, \overline{q}_1)$ ортогональны; в частности, при $p \neq q$ подпространство $G(p, \overline{q})$ вполне изотропно. Показать, что подпространство $G(p, \overline{p})$ нулевое или неизотропное и что при $p \neq q$ ни один ненулевой вектор из $G(p, \overline{q})$ не ортогонален к $G(q, \overline{p})$ (воспользоваться тем, что форма Ф невырождена); вывести отсюда, что при $p \neq q$ подпространства $G(p, \overline{q})$ и $G(q, \overline{p})$ вполне изотропны и имеют одинаковую размерность и их сумма $G(p, \overline{q}) + G(q, \overline{p})$ неизотропна.

в) Предположим, что автоморфизм J отличен от тождественного, характеристика поля A не равна 2 и $u^* = u$. Пусть $\mathfrak{M}$ — множество *неизотропных* подпространств $M \subset G(p, \overline{p})$, устойчивых относительно эндоморфизма u (и, следовательно, подмодулей $A[X]$-модуля E_u (гл. VII, § 5, n° 1)). Показать, что всякий минимальный элемент M множества $\mathfrak{M}$ является *неразложимым* подмодулем модуля E_u (гл. VII, § 4, n° 7). (Предположить, что M есть прямая сумма неразложимого подмодуля M_1 и некоторого подмодуля $M_2 \neq \{0\}$, и рассмотреть минимальные многочлены p^h и p^k сужений эндоморфизма u на M_1 и M_2 соответственно, считая, что $h \geqslant k$. Заметить, что модуль M_1 должен быть изотропным и что всякий его элемент $z \neq 0$ такой, что $p(u)z = 0$, ортогонален к M_1 (воспользоваться тем, что всякий подмодуль модуля M_1 моногенный); записать, что $z = (p(u))^{h-1}x$ и что z не ортогонален к M_2, и вывести отсюда, что $k = h$. Показать затем, что в M_2 имеется неразложимый подмодуль N_2 такой, что сумма

$M_1 + N_2$ неизотропна, и минимальным многочленом сужения эндоморфизма u на N_2 является p^h; вывести отсюда, что $M_2 = N_2$. Наконец, взяв элемент $y \in M_2$, не ортогональный к z, рассмотреть в модуле M подмодуль P, порожденный элементом $w = x + \lambda y$, где $\lambda \in A$, и показать, что элемент λ можно выбрать так, чтобы модуль был неизотропным (доказав для этого, что $\Phi((p(u))^{h-1}w, w) \neq 0$); это приводит к противоречию.)

г) Вывести из утверждения в), что подпространство $G(p, \overline{p})$ является прямой суммой попарно ортогональных неразложимых подмодулей H_i. Показать, что если минимальный многочлен сужения эндоморфизма u на H_i равен p^h и степень многочлена p равна d, то в H_i имеется вполне изотропное подпространство размерности $d\left[\frac{h}{2}\right]$. Разобрать случай, когда пространство E не содержит ненулевых изотропных векторов (см. § 7, n° 3).

д) Сформулировать и доказать утверждения, аналогичные в) и г), в случаях, когда $u^* = -u$ или $u^*u = 1$.

е) Привести пример, в котором $n = 4$, Φ — симметрическая форма индекса 2, $p = \overline{p} = X - 1$, эндоморфизм u нормален, $E = G(p, \overline{p})$, но E не является прямой суммой минимальных подмодулей из множества $\mathfrak{M}$ и существует вектор, являющийся собственным для эндоморфизма u, но не для u^* (см. § 7, n° 3).

13) В предположениях упражнения 2 будем считать дополнительно, что пространство E имеет счетный базис (e_n). Пусть F — вполне изотропное (соответственно вполне сингулярное) подпространство в E такое, что $F^{00} = F$; показать, что существует вполне изотропное (соответственно вполне сингулярное) подпространство F' такое, что: 1° $F \cap F' = \{0\}$; 2° в подпространствах F и F' существуют базисы $(a_m)_{m\in I}$ и $(a'_m)_{m\in I}$ такие, что для любой пары индексов $\Phi(a_i, a'_j) = \delta_{ij}$ (I — отрезок множества N с началом в 0); 3° $(F + F')^{00} = F + F'$, и пространство E является прямой суммой подпространств $F + F'$ и $(F + F')^0$. (Построить по индукции возрастающую последовательность (L_n) неизотропных подпространств с объединением E и такую, что $\dim L_{n+1} - \dim L_n = 2$; к каждому L_n применить предложение 2 n° 2; для построения этой последовательности для всякого n рассмотреть наименьшее целое число k такое, что $e_k \in L_n$, и воспользоваться упражнением 9б) § 1.)

14) Пусть A — тело характеристики 2, E — векторное пространство конечной размерности n над телом A, Φ — невырожденная эрмитова форма на E, не обязательно удовлетворяющая условию (T).

а) Показать, что множество V элементов $x \in E$ таких, что $\Phi(x, x)$ имеет вид $\alpha + \overline{\alpha}$, является векторным подпространством в E.

б) Пусть $V_1 = V \cap V^0$, $q = \dim V_1$, V_2 — дополнение V_1 относительно V, V_3 — дополнение V_1 относительно V^0. Показать, что под-

пространство $(V_2 + V_3)^0 = V_2^0 \cap V_3^0$ имеет базис $(e_i)_{1 \leqslant i \leqslant 2q}$ такой, что векторы $e_1, \ldots, e_q$ образуют базис подпространства V_1 и при $1 \leqslant i \leqslant q$, $1 \leqslant j \leqslant q$ выполняется равенство $\Phi(e_i, e_{q+j}) = \delta_{ij}$.

в) Пусть $G(\Phi)$ — группа метрических автоморфизмов пространства E (относительно формы Φ). Показать, что для любого $u \in G(\Phi)$ равенство $u(x) = x$ выполняется для всех $x \in V^0$.

г) Для любого $u \in G(\Phi)$ имеем равенство $u(V) = V$; пусть u_V — сужение автоморфизма u на V и G_V — группа, состоящая из всех u_V. Показать, что: 1° ядро гомоморфизма $u \to u_V$ группы $G(\Phi)$ на G_V коммутативно; 2° если Φ_2 — сужение формы Φ на V_2 и $G(\Phi_2)$ — группа метрических автоморфизмов V_2 относительно Φ_2, то существует гомоморфизм группы G_V на $G(\Phi_2)$, ядро которого коммутативно (воспользоваться упражнениями б) и в)).

д) Предположим, что A коммутативно и автоморфизм J тождественный; пусть E — векторное пространство над полем A размерности 3, $(e_i)_{1 \leqslant i \leqslant 3}$ — некоторый базис пространства E, Φ — невырожденная симметрическая билинейная форма на E, матрица которой относительно базиса (e_i) равна

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Показать, что все изотропные векторы пространства E содержатся в гиперплоскости, порожденной векторами e_2 и e_3 (см. упражнение 4а)). Привести пример плоскости, изотропной, но содержащей лишь одну изотропную прямую (см. упражнение 2а)). Показать, что не существует автоморфизма $u \in G(\Phi)$ такого, что $u(e_1) = e_1 + e_2$, хотя $\Phi(e_1, e_1) = \Phi(e_1 + e_2, e_1 + e_2)$.

§ 5. Некоторые свойства знакопеременных билинейных форм

1. *Приведение знакопеременных билинейных форм*

Теорема 1. *Пусть A — (коммутативное) кольцо главных идеалов, E — свободный A-модуль конечной размерности n, и Φ — знакопеременная билинейная форма на модуле E. Тогда существуют базис $(e_i)_{1 \leqslant i \leqslant n}$ модуля E и четное число $2r \leqslant n$ такие, что*

1° $\Phi(e_1, e_2) = \alpha_1$, $\Phi(e_3, e_4) = \alpha_2$, $\ldots$, $\Phi(e_{2r-1}, e_{2r}) = \alpha_r$,

где α_i — ненулевые элементы кольца A, и α_i делит α_{i+1} при $i = 1, \ldots, r-1$.

2° *Все остальные элементы $\Phi(e_i, e_j)$, где $i \leqslant j$, равны нулю.*

Идеалы $A\alpha_i$ $(i = 1, \ldots, r)$ *однозначно определяются этими двумя условиями. Подмодуль* E^0 *модуля* E, *ортогональный к* E, *порождается элементами* $e_{2r+1}, \ldots, e_n$.

Доказательство проведем индукцией по размерности n пространства E. Для $n = 0$ теорема очевидна. Если $\Phi = 0$, то она также очевидна; предположим, что $\Phi \neq 0$.

Обозначим через f линейное отображение d_Φ модуля E в E^*, ассоциированное справа с формой Φ (§ 1, n° 1); тогда $f(E)$ будет ненулевым подмодулем модуля E^*, который является свободным модулем размерности n. Пусть $A\alpha_1$ — наибольший инвариантный множитель подмодуля $f(E)$ относительно E^* (гл. VII, § 4, n° 2, теорема 1); известно (там же), что в модуле E^* существуют базис $(e'_1, a'_2, \ldots, a'_n)$ и элемент $f(e_2) \in f(E)$ такие, что $f(e_2) = \alpha_1 e'_1$. Пусть $(e_1, a_2, \ldots, a_n)$ — сопряженный к $(e'_1, a'_2, \ldots, a'_n)$ базис модуля E (отождествленного с E^*); тогда

$$\Phi(e_1, e_2) = -\Phi(e_2, e_1) = \langle e_1, f(e_2)\rangle = \alpha_1. \tag{1}$$

Пусть P — подмодуль $Ae_1 + Ae_2$ модуля E. Убедимся, что E является *прямой суммой* подмодулей Ae_1, Ae_2 и P^0, ортогонального к P. Для этого достаточно доказать, что для любого $x \in E$ существуют однозначно определенные элементы ξ_1 и ξ_2 кольца A такие, что $x - \xi_1 e_1 - \xi_2 e_2 \in P^0$, то есть

$$\Phi(e_1, x - \xi_1 e_1 - \xi_2 e_2) = 0, \qquad \Phi(e_2, x - \xi_1 e_1 - \xi_2 e_2) = 0.$$

В силу (1) эти условия можно переписать так:

$$\langle e_1, f(x)\rangle = \xi_2 \alpha_1, \qquad \langle e_2, f(x)\rangle = -\xi_1 \alpha_1.$$

Но, как известно (там же), образ подмодуля $f(E)$ для любой линейной формы на модуле E^* содержится в идеале $A\alpha_1$; иными словами, все значения $\Phi(x, y) = \langle x, f(y)\rangle$ входят в $A\alpha_1$, отсюда следует существование и единственность элементов ξ_1 и ξ_2. Таким образом, P^0 — свободный модуль ранга $n - 2$; следовательно, по предположению индукции, в P^0 существует базис $(e_3, e_4, \ldots, e_n)$, удовлетворяющий доказываемым условиям. Чтобы убедиться, что построенный таким образом базис $(e_1, \ldots, e_n)$ модуля E также удовлетворяет этим условиям, достаточно показать, что α_1 делит α_2; однако это следует из того, что все значения $\Phi(x, y)$ являются кратными элемента α_1. Ясно, что $e_{2r+1}, \ldots, e_n$ порождают модуль E^0. Наконец, если базис (e'_i) сопряжен к (e_i), то $f(e_{2j-1}) = -\alpha_j e'_{2j}$

и $f(e_{2j}) = \alpha_j e'_{2j-1}$ для $j=1, \ldots, r$, и $f(e_k)=0$ для $k = 2r+1, \ldots, n$; идеалы $A\alpha_1$, $A\alpha_1$, $A\alpha_2$, $A\alpha_2$, ..., $A\alpha_r$, $A\alpha_r$ будут, следовательно, инвариантными множителями модуля $f(E)$ относительно E^*, что доказывает их единственность (гл. VII, § 4, n° 2, теорема 1).

Следствие 1. *Пусть A — поле, E — векторное пространство конечной размерности n над полем A, и Φ — знакопеременная билинейная форма на пространстве E. Тогда существуют базис $(e_i)_{1\leqslant i\leqslant n}$ пространства E и четное число $2r\leqslant n$ такие, что*

$$\Phi\Big(\sum_{i=1}^{n}\xi_i e_i,\ \sum_{i=1}^{n}\eta_i e_i\Big)=\sum_{j=1}^{r}(\xi_{2j-1}\eta_{2j}-\xi_{2j}\eta_{2j-1}). \qquad (2)$$

В частности, форма Φ имеет четный ранг $2r$.

Базис, обладающий свойством (2), называется *симплектическим.*

Замечание. Это утверждение легко следует также из предложения 3 § 4, n° 2, и его следствия 1, так как, в обозначениях этого предложения, H обязательно равно $\{0\}$, поскольку форма Φ знакопеременная.

Следствие 2. *Пусть A — поле, E — векторное пространство конечной размерности n над полем A. Для всякого бивектора $z \in \bigwedge^2 E$ существует базис $(e_i)_{1\leqslant i\leqslant n}$ пространства E такой, что*

$$z = e_1\wedge e_2 + e_3\wedge e_4 + \ldots + e_{2r-1}\wedge e_{2r} \qquad (2r\leqslant n).$$

В самом деле, достаточно заметить, что бивектор канонически отождествляется с некоторой знакопеременной билинейной формой на модуле E^* (гл. III, § 8, n° 2), и применить к этой форме следствие 1.

В переводе на матричный язык следствие 1 означает:

Следствие 3. *Пусть A — поле, R — знакопеременная квадратная матрица над полем A. Ранг матрицы R равен четному числу $2r$, и существует обратимая матрица P над полем A такая, что*

$${}^tPRP=\begin{pmatrix} 0 & I_r & 0\\ -I_r & 0 & 0\\ 0 & 0 & 0\end{pmatrix}.$$

З а м е ч а н и е. Если A — произвольное коммутативное кольцо и R — знакопеременная квадратная матрица *нечетного* порядка над кольцом A, то $\det R = 0$. В случае, когда A — поле, это получается из следствия 3. Непосредственно доказать это утверждение в случае, когда A является полем характеристики $\neq 2$, можно следующим образом: так как ${}^tR = -R$, то $\det R = \det {}^tR = (-1)^n \det R$, откуда $2 \det R = 0$. Но тогда, поскольку определитель знакопеременной матрицы (α_{ij}) является многочленом от α_{ij}, $i < j$, с целыми коэффициентами, наше утверждение верно для любого коммутативного кольца A в силу принципа продолжения алгебраических тождеств (гл. IV, § 2, n° 5, схолия).

2. *Пфаффиан знакопеременной матрицы*

Пусть A — поле характеристики 0 и $R = (\alpha_{ij})$ — знакопеременная матрица *четного* порядка $2m$ над полем A. Обозначим через E векторное пространство A^{2m}, через (e_i) $(i = 1, \ldots, 2m)$ — его канонический базис и через e — элемент $e_1 \wedge e_2 \wedge \ldots \wedge e_{2m}$ внешней степени $\bigwedge^{2m} E$. m-я внешняя степень бивектора $u = \sum_{i<j} \alpha_{ij} e_i \wedge e_j \in \bigwedge^2 E$ имеет вид αe, где α — элемент кольца A, который мы сейчас вычислим. Элемент $\bigwedge^m u$ является суммой членов вида

$$\alpha_{h_1k_1}\alpha_{h_2k_2} \ldots \alpha_{h_mk_m} e_{h_1} \wedge e_{k_1} \wedge e_{h_2} \wedge e_{k_2} \wedge \ldots \wedge e_{h_m} \wedge e_{k_m}, \qquad (3)$$

где $h_j < k_j$ при $j = 1, \ldots, m$. Такой член равен нулю, если в него входят два одинаковых e_j, то есть если множество $\{h_1, k_1, \ldots, h_m, k_m\}$ не совпадает с $\{1, 2, \ldots, 2m\}$. Кроме того, если в выражении (3) одновременно поменять местами e_{h_r} с $e_{h_{r+1}}$ и e_{k_r} с $e_{k_{r+1}}$, то произведение не изменится; следовательно, оно не изменится и при любой перестановке *пар* $(h_1, k_1), \ldots, (h_m, k_m)$. Рассмотрим теперь множества (не упорядоченные) $S = \{(h_1, k_1), \ldots, (h_m, k_m)\}$ пар (h_j, k_j), в которых $1 \leqslant h_j < k_j \leqslant 2m$ для $j = 1, 2, \ldots, m$; пусть $\mathscr{C}$ — множество этих пар. Для $S \in \mathscr{C}$ положим

1° $\varepsilon(S) = 0$, если $\{h_1, k_1, \ldots, h_m, k_m\} \neq \{1, 2, \ldots, 2m\}$.

2° В противоположном случае $\varepsilon(S) = 1$ или $\varepsilon(S) = -1$ в зависимости от того, является ли четной или нечетной перестановка, переводящая h_j в $2j - 1$, а k_j в $2j$ $(j = 1, \ldots, m)$.

Тогда предыдущие рассуждения показывают, что элемент $\bigwedge^m u$ равен

$$m! \sum_{S \in \mathfrak{S}} \varepsilon(S) \Big(\prod_{(h,k) \in S} a_{hk} \Big) e. \tag{4}$$

Введем теперь $m(2m-1)$ переменных X_{hk} с индексами, соответствующими парам (h, k) таким, что $1 \leqslant h < k \leqslant 2m$, и обозначим через P многочлен от переменных X_{hk} над кольцом Z, определяемый формулой

$$P((X_{hk})) = \sum_{S \in \mathfrak{S}} \varepsilon(S) \Big(\prod_{(h,k) \in S} X_{hk} \Big). \tag{5}$$

Тогда будет выполнено равенство

$$\bigwedge^m u = m!\, P((a_{hk}))\, e. \tag{6}$$

Определение 1. *Пусть* $R = (\alpha_{ij})$ $(i, j = 1, \ldots, 2m)$ — *знакопеременная матрица четного порядка* $2m$ *над коммутативным кольцом* A. *Пфаффианом* $\mathrm{Pf}(R)$ *матрицы* R *называется элемент* $P((\alpha_{hk}))$ *кольца* A, *где* $1 \leqslant h < k \leqslant 2m$.

Пример. Пусть

$$\alpha_{12} = -\alpha_{21} = \beta_1,\ \alpha_{34} = -\alpha_{43} = \beta_2,\ \ldots,\ \alpha_{2m-1,\,2m} = -\alpha_{2m,\,2m-1} = \beta_m,$$

а все остальные α_{ij} равны нулю (см. теорему 1). Тогда пфаффиан матрицы $R = (\alpha_{ij})$ равен $\beta_1 \beta_2 \ldots \beta_m$.

Предложение 1. *Пусть* R — *знакопеременная матрица четного порядка* $2m$ *над коммутативным кольцом* A, *и* P — *произвольная квадратная матрица порядка* $2m$ *над кольцом* A.

Тогда

$$\mathrm{Pf}({}^tPRP) = \det P \cdot \mathrm{Pf}(R). \tag{7}$$

В самом деле, пусть сначала A — поле характеристики 0. Положим $R = (\alpha_{ij})$, $P = (\beta_{ij})$. Матрице R поставим в соответствие бивектор u:

$$u = \sum_{i<j} \alpha_{ij} e_i \wedge e_j = \frac{1}{2} \sum_{1 \leqslant i,\, j \leqslant 2m} \alpha_{ij} e_i \wedge e_j$$

внешней степени $\bigwedge^2 A^{2m}$ и обозначим через (e_i) канонический базис пространства A^{2m}, матрицу P будем рассматривать как матрицу относительно базиса (e_i) некоторого эндоморфизма f пространства A^{2m}. Тогда бивектор $(\bigwedge^2 f)(u)$ равен $\frac{1}{2} \sum_{i,\,j,\,s,\,t} \beta_{is} \alpha_{ij} \beta_{jt} e_s \wedge e_t$,

то есть соответствует, по указанному правилу, матрице ${}^tP \cdot R \cdot P$. Так как продолжение $\bigwedge f$ эндоморфизма f на внешнюю алгебру $\bigwedge A^{2m}$ является эндоморфизмом этой алгебры (гл. III, § 5, n° 9), имеем равенство $\overset{m}{\bigwedge}((\overset{2}{\bigwedge} f)(u)) = (\overset{2m}{\bigwedge} f)(\overset{m}{\bigwedge} u)$. Но $\overset{2m}{\bigwedge} f$ — это гомотетия относительно $\det f$, так что из формулы (6) и определения 1 следует равенство $m!\ \mathrm{Pf}({}^tPRP) = m!\,(\det P)\,\mathrm{Pf}(R)$, то есть в рассмотренном случае равенство (7) верно. Доказательство в общем случае получается, если заметить, что обе части равенства (7) являются многочленами с целыми коэффициентами от элементов матриц R и P (гл. IV, § 2, n° 5, схолия).

Предложение 2. *Для всякой знакопеременной матрицы R четного порядка $2m$ над коммутативным кольцом A выполняется равенство*

$$\det R = (\mathrm{Pf}(R))^2. \tag{8}$$

В самом деле, обе части равенства (8) являются многочленами с целыми коэффициентами от элементов матрицы R, так что, в силу принципа продолжения алгебраических тождеств (гл. IV, § 2, n° 5, схолия), достаточно провести доказательство лишь в случае, когда A — поле характеристики 0 и $\det R \neq 0$. Пусть P — произвольная обратимая квадратная матрица порядка $2m$ над полем A. Тогда $\det({}^tPRP) = (\det P)^2 \det R$ и $\mathrm{Pf}({}^tPRP) = (\det P)\,\mathrm{Pf}(R)$ (предложение 1). Поэтому равенство (8) достаточно доказать для матрицы ${}^tPRP$. Благодаря следствию 1 из теоремы 1 матрицу P можно выбрать так, что ${}^tPRP$ будет иметь вид (α_{ij}), где

$$\alpha_{12} = -\alpha_{21} = 1,\ \ldots,\ \alpha_{2m-1,\,2m} = -\alpha_{2m,\,2m-1} = 1,$$

а все остальные α_{ij} равны нулю (см. пример). Но тогда определитель этой матрицы, как и ее пфаффиан, равен 1, что и заканчивает доказательство.

3. *Симплектическая группа*

Будем предполагать, что кольцо A *коммутативно*. Пусть Φ — знакопеременная билинейная форма на модуле E. Автоморфизмы модуля E, оставляющие форму Φ инвариантной, называются *симплектическими автоморфизмами* (или *симплектическими пре-*

образованиями) модуля E относительно формы Ф. Эти автоморфизмы образуют группу, называемую *симплектической группой*, ассоциированной с формой Ф. Иногда эта группа обозначается Sp (Ф).

Рассмотрим, в частности, на модуле $E = A^{2m}$ знакопеременную билинейную форму Φ_0, матрица которой в каноническом базисе (e_i) модуля E имеет вид

$$R_m = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}.$$

Симплектические автоморфизмы, ассоциированные с формой Φ_0, называются просто симплектическими автоморфизмами, а симплектическая группа, ассоциированная с Φ_0, называется симплектической группой *от* $2m$ *переменных* (над кольцом A). Эта группа обозначается Sp $(2m, A)$ или $\mathrm{Sp}_{2m}(A)$. Матрица симплектического автоморфизма относительно канонического базиса (e_i) называется *симплектической матрицей*. Всякая симплектическая матрица обратима и по формуле (48) § 1, n° 10, удовлетворяет соотношению

$$^tAR_mA = R_m. \tag{9}$$

Обратно, если квадратная матрица порядка $2m$ удовлетворяет (9), то она симплектическая. В самом деле, достаточно показать, что она обратима; однако в силу предложения 1 n° 2 и (9) $\mathrm{Pf}(R_m) = \mathrm{Pf}(^tAR_mA) = (\det A)\,\mathrm{Pf}(R_m)$, то есть $\det A = 1$.

Одновременно мы доказали следующее утверждение:

Предложение 3. *Определитель симплектической матрицы равен* 1.

Если A — поле и Ф — невырожденная билинейная форма на векторном пространстве E четной размерности $2m$ над телом A, то ассоциированная с формой Ф симплектическая группа *изоморфна* Sp $(2m, A)$. Это получается из следствия 1 теоремы 1.

Упражнения. 1) Пусть A — коммутативное кольцо главных идеалов, E — свободный A-модуль конечной размерности n, Ф — знакопеременная билинейная форма на E; идеалы $A\alpha_i$ $(1 \leqslant i \leqslant r)$, определенные в теореме 1 n° 1, называются *инвариантными множителями* формы Ф.

а) Пусть F — подмодуль E, Φ_F — сужение формы Φ на F и $A\beta_i$ $(1 \leqslant i \leqslant s)$ — инвариантные множители формы Φ_F (β_i делит β_{i+1}). Показать, что $s \leqslant r$ и для $1 \leqslant i \leqslant s$ элемент β_i кратен α_i. (Свести доказательство к случаю $r = s = \frac{n}{2}$ и воспользоваться упражнениями 9б) и 9в) гл. VII, § 4.)

б) Пусть E_1 — второй свободный A-модуль конечной размерности, Φ_1 — знакопеременная билинейная форма на E_1, $A\gamma_1, \ldots, A\gamma_s$ — ее инвариантные множители (γ_i делит γ_{i+1}). Для того чтобы форма Φ_1 была обратным образом формы Φ при некотором линейном отображении модуля E_1 в E, необходимо и достаточно, чтобы $s \leqslant r$ и элемент γ_i был кратным α_i для $1 \leqslant i \leqslant s$. (Использовать а) и предложение 4, гл. VII, § 4, n° 5.)

в) Пусть F, G — подмодули модуля E такие, что F^0 (соответственно G^0) является дополнением F (соответственно G) в E. Показать, что если сужения формы Φ на F и G эквивалентны, то эквивалентны и ее сужения на F^0 и G^0, и что существует автоморфизм модуля E, оставляющий инвариантной форму Φ и переводящий F в G.

г) Привести пример двух подмодулей F, G модуля E, имеющих размерность 2, обладающих дополнениями в E и таких, что ограничения Φ_F и Φ_G эквивалентны, но не существует автоморфизма модуля E, оставляющего форму Φ инвариантной и переводящего F в G (взять $n = 4$).

2) Пусть Φ — знакопеременная билинейная форма на конечномерном векторном пространстве E. Показать, что для любого векторного подпространства M пространства E разность $\dim M - \dim (M \cap M^0)$ *четная*. (Рассмотреть сначала случай, когда форма Φ невырождена.)

*3) Пусть E — векторное пространство четной размерности $n = 2m$ над полем A, и пусть Φ и Ψ — знакопеременные билинейные формы на E; предположим, что форма Ψ не вырождена. Пусть u и v — линейные отображения модуля E в E^*, ассоциированные справа с формами Φ и Ψ соответственно; отображение v есть изоморфизм модуля E на E^*; положив $w = v^{-1} \circ u$, получим, что w — эндоморфизм пространства E.

а) Положим $M_0 = E$ и, по индукции, $M_{k+1} = w(M_k)$ для $k \geqslant 0$. Пусть M'_k — подпространство, ортогональное к M_k относительно Φ. Показать, что M_{k+1} — подпространство, ортогональное к M'_k относительно Ψ.

б) Пусть n_0 — размерность подпространства M'_0; положим $m_0 = 0$ и обозначим через m_k, $k \geqslant 1$, размерность подпространства $M_k \cap M'_0$. Показать, что размерность подпространства M_k, $k \geqslant 1$, равна $n - n_0 - (m_1 + \ldots + m_{k-1})$, а размерность M'_k, $k \geqslant 1$, равна $n_0 + (m_1 + \ldots + m_k)$.

в) Показать, что при любом $k \geqslant 0$ размерность подпространства $M_k \cap M'_k$ равна $m_k + m_{k+1} + \ldots + m_{2k}$, а размерность $M'_k \cap M_{k+1}$

равна $m_{k+1} + m_{k+2} + \ldots + m_{2k+1}$ (для вычисления с помощью индукции по k размерностей подпространств $M'k \cap M_{2k+1-k}$ применить упражнение 2б) § 3).

г) Вывести из упражнения в), что числа m_k *четные* (использовать упражнение 2).

д) Получить из г), что число элементарных делителей эндоморфизма w, соответствующих характеристическому корню $\lambda = 0$ и имеющих данную степень, *четно* (см. гл. VII, § 5, упражнение 20).

4) Пусть E — векторное пространство над полем A, имеющее счетный базис $(e_n)_{n \geqslant 1}$, Φ — невырожденная знакопеременная форма на E. Показать, что в пространстве E существует такой базис (a_n), что $\Phi(a_{2n-1}, a_{2n}) = 1$ для любого $n \geqslant 1$ и $\Phi(a_i, a_j) = 0$ для любой другой пары индексов с $i < j$ (рассуждать, как в упражнении 13 § 4).

5) Показать, что для всякой знакопеременной матрицы $X = (x_{ij})$ четного порядка $n = 2m$ над коммутативным кольцом и для всякого инденса i справедливо равенство $\mathrm{Pf}(X) = \sum_{j=1}^{n} (-1)^{i+j-1} \mathrm{Pf}(X_{ij})\, x_{ij}$, где X_{ij} — матрица порядка $n - 2$, получаемая из X вычеркиванием строк и столбцов с номерами i и j.

6) Пусть M — квадратная матрица порядка m над коммутативным кольцом. Положим

$$R = \begin{pmatrix} 0 & M \\ -{}^tM & 0 \end{pmatrix}.$$

Показать, что $\mathrm{Pf}(R) = \det M$ (используя формулу (7), доказать сначала это равенство в случае, когда матрица M обратима).

7) Пусть A — поле, $\mathfrak{A}(A)$ — множество знакопеременных матриц порядка $2m$ над полем A; пусть I — такое отображение множества $\mathfrak{A}(A)$ в A, что для любой матрицы $R \in \mathfrak{A}(A)$ и любой матрицы P порядка $2m$ над полем A выполняется равенство $I({}^tPRP) = (\det P)^h I(R)$, где h — целое рациональное число. Показать, что $I(R) = c\,(\mathrm{Pf}(R))^h$, где $c \in A$ (воспользоваться формулой (7) и теоремой 1 n° 1).

8) Пусть P, Q — знакопеременные квадратные матрицы четного порядка $2m$ над коммутативным кольцом A. Пусть $\varphi(X) = \mathrm{Pf}(P - XQ)$; показать, что если матрица Q обратима, то $\varphi(Q^{-1}P) = 0$. (Рассмотреть сначала случай, когда A — поле; затем из упражнения 3 вывести, что минимальный многочлен матрицы $Q^{-1}P$ делит $\varphi(X)$ — для этого перейти к алгебраически замкнутому расширению поля A и заметить, что φ^2 с точностью до скалярного множителя совпадает с характеристическим многочленом матрицы $Q^{-1}P$.)

*9) Пусть E — векторное пространство размерности n над полем A, Φ — знакопеременная билинейная форма на E, Ψ — эрмитова полуторалинейная форма на E (относительно некоторого инволютивного автоморфизма поля A), P и Q — матрицы форм Φ и Ψ соответственно относительно одного и того же базиса пространства E.

а) Предположим, что форма Φ не вырождена. Показать, что число элементарных делителей матрицы $Q^{-1}P$, соответствующих характеристическому корню 0 и имеющих одну и ту же *четную* степень, четно (метод тот же, что и в упражнении 3).

б) Предположим, что форма Φ не вырождена (отсюда следует, что n четно). Показать, что число элементарных делителей матрицы $P^{-1}Q$, соответствующих характеристическому корню 0 и имеющих одну и ту же *нечетную* степень, четно (метод тот же).

10) Пусть $\omega_{2m}(\boldsymbol{F}_q)$ — порядок симплектической группы $\mathrm{Sp}(2m, \boldsymbol{F}_q)$ над конечным полем $\boldsymbol{F}_q$. Показать, что $\omega_{2m}(\boldsymbol{F}_q) = h_{2m}\omega_{2m-2}(\boldsymbol{F}_q)$, где h_{2m} — число пар векторов (x, y) из $\boldsymbol{F}_q^{2m}$, удовлетворяющих условию $\Phi_0(x, y) = 1$ (обозначения из n° 3); вывести отсюда равенство

$$\omega_{2m}(\boldsymbol{F}_q) = (q^{2m}-1)\,q^{2m-1}\,(q^{2m-2}-1)\,q^{2m-3}\ldots(q^2-1)\,q.$$

11) Пусть A — поле. Показать, что всякое преобразование u, принадлежащее симплектической группе $\mathrm{Sp}(2m, A)$, является произведением сдвигов, принадлежащих этой группе (называемых *симплектическими сдвигами*; см. § 4, упражнение 6). (Провести индукцию по m, показав, что если векторы x и y из $E = A^{2m}$ не ортогональны, то существует произведение v симплектических сдвигов такое, что vu оставляет x и y инвариантными.) Получить отсюда новое доказательство предложения 3 n° 3.

12) Пусть A — поле, E — векторное пространство четной размерности $n = 2m$ над полем A, Φ — невырожденная знакопеременная билинейная форма на E. Показать, что для любого подобия u относительно формы Φ (§ 6, n° 5) с коэффициентом α выполняется равенство $\det u = \alpha^m$ (воспользоваться формулой (7)).

*13) Предположим, что поле A имеет характеристику 0, E — векторное пространство размерности $2m$ над полем A, Φ — невырожденная знакопеременная билинейная форма на E. Отождествим форму $\hat{\Phi}$, обратную к Φ, с бивектором $\Gamma \in \bigwedge^2 E$. Тогда для всякого симплектического базиса $(e_i)_{1\leqslant i\leqslant 2m}$ пространства E (относительно формы Φ), занумерованного таким образом, чтобы $\Phi(e_i, e_j) = \Phi(e_{m+i}, e_{m+j}) = 0$, $\Phi(e_i, e_{m+j}) = \delta_{ij}$ $(1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant m)$, выполняется равенство

$$\Gamma = e_1 \wedge e_{m+1} + e_2 \wedge e_{m+2} + \ldots + e_m \wedge e_{2m}.$$

Ненулевой разложимый p-вектор $z \in \bigwedge^p E$ называется *изотропным* (соответственно *вполне изотропным*) относительно Φ, если векторное подпространство V_z, соответствующее z (гл. III, § 7, n° 3), изотропно (соответственно вполне изотропно).

а) Пусть z — ненулевой разложимый p-вектор и $2r$ — размерность дополнения подпространства $V_z \cap V_z^0$ в V_z. Показать, что $m - p + r$ есть наибольшее из целых чисел h, для которых

$z \wedge \Gamma^h \neq 0$, где Γ^h — h-я внешняя степень бивектора Γ во внешней алгебре $\bigwedge E$ (воспользоваться предложением 2 § 4, n° 2).

б) Показать, что всякий бивектор $x \in \overset{2}{\bigwedge} E$ может быть записан в виде $\lambda\Gamma + x_1$, где λ — скаляр, а x_1 — линейная комбинация вполне изотропных разложимых бивекторов. (Свести доказательство к случаю, когда бивектор x разложим, и заметить, что если базис (e_i) симплектический, то бивектор $(e_1+e_2) \wedge (e_{m+1} - e_{m+2})$ вполне изотропен.)

в) Пусть $p \leqslant m$. Показать, что всякий p-вектор $z \in \overset{p}{\bigwedge} E$ может быть записан в виде $z = x \wedge \Gamma + z_1$, где x — $(p-2)$-вектор, а z_1 — линейная комбинация вполне изотропных разложимых p-векторов. (Свести доказательство к случаю, когда p-вектор z разложим, и применить индукцию по p. Таким же образом свести все к случаю, когда $z = e_1 \wedge e_2 \wedge \ldots \wedge e_{p-1} \wedge e_{m+p-1}$, где (e_i) — симплектический базис, и для $0 \leqslant i \leqslant m-p$ рассмотреть бивекторы

$$(e_{p-1}+e_{p+i}) \wedge (e_{m+p-1}-e_{m+p+i}).)$$

г) Пусть $1 \leqslant p \leqslant m$. Показать, что всякий $(m+p)$-вектор $z \in \overset{m+p}{\bigwedge} E$ может быть записан в виде $z = y \wedge \Gamma^p$, где y — $(m-p)$-вектор. (Свести доказательство к случаю, когда z разложим; рассмотреть два случая: $r = p$ и $r > p$, где $2r$ — размерность дополнения подпространства $V_z \cap V_z^0$ относительно V_z; во втором случае применить индукцию по r — так же, как в упражнении в).) Вывести отсюда, что отображение $y \to y \wedge \Gamma^p$ степени $\overset{m-p}{\bigwedge} E$ в $\overset{m+p}{\bigwedge} E$ биективно (заметить, что оба пространства имеют одну и ту же размерность). Показать, что если $(m-p)$-вектор y разложим, то $z = y \wedge \Gamma^p$ разложим и $V_z = V_y^0$.

д) Вывести из г), что при $p \leqslant m$ подпространство $\overset{p}{\bigwedge} E$ есть прямая сумма однородной компоненты степени p двустороннего идеала с, порожденного в $\bigwedge E$ элементом Γ, и подпространства R_p, состоящего из p-векторов z_1 таких, что $z_1 \wedge \Gamma^{m-p+1} = 0$ (для $z \in \overset{p}{\bigwedge} E$ применить г) к $(2m-p+2)$-вектору $z \wedge \Gamma^{m-p+1}$). Используя в), показать, что подпространство R_p порождается вполне изотропными разложимыми p-векторами, и, используя г), показать, что отображение $x \to x \wedge \Gamma$ степени $\overset{p-2}{\bigwedge} E$ в $\overset{p}{\bigwedge} E$ инъективно и размерность R_p равна $\binom{2m}{p} - \binom{2m}{p-2}$.

е) Пусть $p \leqslant m$. Доказать, что p-вектор z тогда и только тогда имеет вид $x \wedge \Gamma$, когда $z \wedge u = 0$ для любого вполне изотропного разложимого m-вектора u. (Показать, что если это условие выполнено и $z \in R_p$, то $z \wedge y = 0$ для любого $(2m-p)$-вектора y; для этого представить y в виде $x \wedge \Gamma^{m-p}$, где x — p-вектор, затем

применить к x утверждение в) и заметить, что если x_1 — вполне изотропный разложимый p-вектор, то $(2m-p)$-вектор $x_1 \wedge \Gamma^{m-p}$ вполне разложим и может быть представлен в виде $u_1 \wedge v_1$, где u_1 — вполне изотропный разложимый m-вектор.)

Пусть $\mathfrak{a}$ — аннулятор идеала $\mathfrak{c}$ в $\bigwedge E$; $\mathfrak{a}$ есть прямая сумма подпространств R_m, $R_{m-1} \wedge \Gamma$, . . , $R_1 \wedge \Gamma^{m-1}$ и $A\Gamma^m$. Показать, что аннулятор идеала $\mathfrak{a}$ в $\bigwedge E$ равен $\mathfrak{c}$ (см. § 2, упражнение 4б)).

ж) Пусть u — симплектический автоморфизм пространства E (относительно Ф) и $\bar{u}$ — его каноническое продолжение до автоморфизма алгебры $\bigwedge E$ (гл. III, § 5, n° 9). Показать, что единственными элементами алгебры $\bigwedge E$, инвариантными относительно всех автоморфизмов $\bar{u}$, являются линейные комбинации элементов 1, Γ, Γ^2, . . ., Γ^m с коэффициентами из A. (Взяв симплектический базис (e_i), записать, что некоторый элемент алгебры $\bigwedge E$ инвариантен относительно симплектических сдвигов (упражнение 11), соответствующих гиперплоскостям, ортогональным к e_i; затем рассмотреть симплектические преобразования u_{ij}, определяемые равенствами $u_{ij}(e_i) = e_j$, $u_{ij}(e_j) = e_i$, $u_{ij}(e_{m+i}) = e_{m+j}$, $u_{ij}(e_{m+j}) = e_{m+i}$, $u_{ij}(e_k) = e_k$ для всех индексов k.)

14) Пусть A — поле характеристики 2, E — векторное пространство A^{2m}; отождествим симплектическую группу $\mathbf{Sp}(2m, A)$ с группой симплектических матриц U, удовлетворяющих, следовательно, условию ${}^tURU = R$, где $R = \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix}$. Положим $D = \begin{pmatrix} 0 & 0 \\ I_m & 0 \end{pmatrix}$: показать, что всякая симплектическая матрица U, для которой матрица $I + U$ обратима, может быть единственным образом записана в виде $({}^tD + S)^{-1}(D + S)$, где матрица S симметрична и $D + S$ обратима, и обратно (см. § 4, упражнение 11).

15) Пусть A — поле, E — векторное пространство размерности $2m$ над полем A, Ф — невырожденная знакопеременная билинейная форма на E.

а) Перенести результаты § 4, упражнения 12 а) и б), на эндоморфизмы u пространства E, удовлетворяющие условию $u^*u = uu^*$ (u^* — эндоморфизм, сопряженный с u относительно формы Ф).

б) Предположим, что $u^* = u$. Пусть M — минимальный элемент множества $\mathfrak{M}$ подпространств, неизотропных, содержащихся в $G(p, p)$ и устойчивых относительно u (обозначения из упражнения 12 § 4). Показать, что M — либо неразложимый подмодуль в E_u, либо сумма двух таких подмодулей, изоморфных друг другу (рассуждать, как в упражнении 12в) § 4). Показать на примерах, что могут осуществиться оба случая (взять $p(X) = X - 1$).

в) Предположим, что $u^* = -u$ и характеристика поля A не равна 2. В тех же обозначениях, пусть p^h — минимальный многочлен сужения эндоморфизма u на M и d — степень многочлена p. Показать, что если $d(h-1)$ нечетно, то M — неразложимый под-

модуль в E_u; напротив, если d $(h-1)$ четно, то модуль M либо неразложим, либо является прямой суммой двух неразложимых подмодулей, изоморфных между собой.

г) Предположим, что $u^*u = 1$ (другими словами, $u \in \mathbf{Sp}(\Phi)$). Если, в обозначениях упражнения в), $p(X)$ не делит $X^{d(h-1)} - 1$ или $p(X) = X - 1$ и $(-1)^h \neq -1$, то M — неразложимый подмодуль в E_u; в противоположном случае подмодуль M либо неразложим, либо является прямой суммой двух неразложимых подмодулей, изоморфных между собой.

§ 6. Некоторые свойства эрмитовых форм

1. *Ортогональные базисы*

Определение 1. *Пусть* Φ — *эрмитова форма на модуле* E. *Базис* (e_i) *модуля* E *называется ортогональным относительно формы* Φ, *если два любых его элемента ортогональны относительно* Φ.

Если, кроме того, $\Phi(e_i, e_i) = 1$ *для любого* i, *то базис* (e_i) *называется ортонормальным.*

Пусть (e_i) — ортогональный базис; положив $\Phi(e_i, e_i) = \alpha_i$, будем иметь равенство

$$\Phi\Big(\sum_i \xi_i e_i,\ \sum_i \eta_i e_i\Big) = \sum_i \xi_i \alpha_i \overline{\eta}_i. \tag{1}$$

Лемма 1. *Пусть* A — *тело и* Φ — *ненулевая эрмитова форма на пространстве* E. *Если все векторы пространства* E *изотропны, то* A — *поле характеристики* 2, *антиавтоморфизм* J — *тождественный и форма* Φ — *знакопеременная.*

В самом деле, развернув равенство $\Phi(x+y,\ x+y) = 0$, получим, учитывая, что, по предположению, $\Phi(x,x) = \Phi(y,y) = 0$, соотношение $\Phi(x, y) = -\overline{\Phi(x, y)}$ для любых $x,\ y \in E$. Поскольку $\Phi \neq 0$, то существуют $x, y \in E$ такие, что $\Phi(x, y) = 1$. Но для любого $\lambda \in A$

$$\Phi(\lambda x, y) = -\overline{\Phi(\lambda x, y)},$$

откуда $\overline{\lambda} = -\lambda$. Положив $\lambda = 1$, получим отсюда, что характеристика тела A равна 2; поэтому соотношение $\overline{\lambda} = -\lambda$ показывает, что антиавтоморфизм J — тождественный, так что тело A — коммутативное, а форма Φ — знакопеременная.

Теорема 1. *Пусть A — тело и E — векторное пространство конечной размерности n над телом A. Тогда для любой эрмитовой формы Φ на пространстве E существует ортогональный базис, за исключением случая, когда выполняется условие*:

(C) *A — поле характеристики 2, антиавтоморфизм J — тождественный, Φ — ненулевая знакопеременная форма.*

Это утверждение очевидно при $n = 0$, и мы проведем индукцию по n. Можно считать, что $\Phi \neq 0$. Если условие (C) не выполнено, то по лемме 1 существует элемент $x \in E$ такой, что $\Phi(x, x) \neq 0$. Пусть H — подпространство пространства E, ортогональное к x. Его размерность $\geqslant n - 1$, но поскольку $x \notin H$, то она в точности равна $n - 1$. Если сужение Ψ формы Φ на подпространство H не удовлетворяет условию (C), то, по предположению индукции, в H существует базис $(e_2, \ldots, e_n)$, ортогональный относительно формы Ψ; положив $e_1 = x$, мы получим ортогональный базис пространства E. Остается рассмотреть случай, когда A — поле характеристики 2, J — тождественный автоморфизм и Ψ — ненулевая знакопеременная форма. Тогда в пространстве H существуют элементы y и z такие, что $\Psi(y, z) \neq 0$; положим $e_1 = x + y$; вектор $x + \lambda z$ ($\lambda \in A$) будет ортогональным к e_1 тогда и только тогда, когда выполняется равенство $0 = \Phi(x + y, x + \lambda z) = \Phi(x, x) + \lambda\Psi(y, z)$. Но это равенство однозначно определяет скаляр λ. Выбрав таким образом λ, мы получим, что $\Phi(x+\lambda z, x + \lambda z) = \Phi(x, x) \neq 0$, так что сужение Ψ' формы Φ на подпространство H' пространства E, ортогональное к e_1, не является знакопеременной формой. Теперь достаточно применить предположение индукции к подпространству H'. Теорема доказана.

Если же условие (C) выполнено, то ортогонального относительно формы Φ базиса, очевидно, не существует.

Следствие 1. *В обозначениях теоремы 1 предположим дополнительно, что условие* (C) *не выполнено, форма Φ невырождена и для всякого $x \in E$ существует элемент $\varrho \in A$ такой, что $\Phi(x, x) = \varrho\bar{\varrho}$. Тогда пространство E обладает относительно Φ ортонормальным базисом.*

В самом деле, пусть (e_i) $(i = 1, \ldots, n)$ — ортогональный базис пространства E. Положим $\Phi(e_i, e_i) = \alpha_i$. Тогда $\alpha_i \neq 0$

($i = 1, \ldots, n$), поскольку форма Φ невырождена. По предположению, существуют элементы $\beta_i \in A$ такие, что $\alpha_i = \beta_i\bar{\beta}_i$ для $i = 1, \ldots, n$, причем $\beta_i \neq 0$. Положив $f_i = \beta_i^{-1}e_i$, будем иметь равенства $\Phi(f_i, f_i) = \beta_i^{-1}\alpha_i\bar{\beta}_i^{-1} = 1$ для любого i и $\Phi(f_i, f_j) = 0$ для $i \neq j$. Следовательно, (f_i) — ортонормальный базис.

Замечание. Предположения этого следствия наверняка выполняются, если J — тождественный автоморфизм и всякий элемент поля A является квадратом некоторого элемента поля A (например, если поле A алгебраически замкнуто).

Следствие 2. *Пусть A — тело и R — эрмитова матрица порядка n и ранга r над телом A. Тогда, если не выполняется условие*

(C′) *A — поле характеристики 2, J — тождественный автоморфизм, R — ненулевая знакопеременная матрица,*

то существует обратимая матрица P над полем A такая, что

$$ {}^tPR\bar{P} = \begin{pmatrix} \alpha_1 & 0 & \ldots & 0 & \ldots & 0 \\ 0 & \alpha_2 & \ldots & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \alpha_r & \ldots & 0 \\ 0 & 0 & \ldots & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & \ldots & 0 \end{pmatrix}, $$

где $\bar{\alpha}_i = \alpha_i \neq 0$ для $i = 1, \ldots, r$.

Предложение 1. *Пусть A — поле, Φ — эрмитова форма на пространстве E, и (x_n) $(n = 1, 2, \ldots)$ — последовательность (конечная или бесконечная) линейно независимых векторов пространства E такая, что для любого n подпространство $E_n = Ax_1 + \ldots + Ax_n$ неизотропно. Пусть, далее, D_{jn} $(j \leqslant n)$ — алгебраическое дополнение элемента $\Phi(x_j, x_n)$ в матрице $(\Phi(x_s, x_t))$ $(s, t = 1, \ldots, n)$. Тогда $D_{nn} \neq 0$ для любого n.*

Положим дополнительно

$$ e_n = \sum_{j=1}^{n} D_{nn}^{-1}D_{jn}x_j. \tag{2} $$

Тогда для любого n система $(e_1, \ldots, e_n)$ *является ортогональным базисом подпространства* E_n *и справедливо равенство*

$$\Phi(e_n, e_n) = D_{nn}^{-1} D_{n+1,\,n+1}. \tag{3}$$

В самом деле, сужение формы Φ на подпространство E_{n-1} невырождено, так что $D_{nn} \neq 0$ (§ 2, предложение 3); заметим теперь, что $D_{11} = 1$, поскольку определитель пустой матрицы равен 1. Из формул (2) следует, прежде всего, что $e_n \equiv x_n \pmod{E_{n-1}}$ для любого n, так что векторы e_n линейно независимы, и что $(e_1, \ldots, e_n)$ является базисом подпространства E_n. Для любого $j < n$ имеем равенство (гл. III, § 6, n° 1, формула (12)); следовательно, вектор e_n ортогонален к E_{n-1} и, в частности, к вектору e_j, $j < n$. С другой стороны, имеем равенства

$$\Phi(e_n, e_n) = \Phi\Big(e_n, \sum_{j=1}^{n} D_{nn}^{-1} D_{jn} x_j\Big) = \Phi(e_n, x_n) =$$

$$= \Phi\Big(\sum_{j=1}^{n} D_{nn}^{-1} D_{jn} x_j,\ x_n\Big) = D_{nn}^{-1} \sum_{j=1}^{n} D_{jn} \Phi(x_j, x_n) = D_{nn}^{-1} D_{n+1,\,n+1}$$

(гл. III, § 6, n° 1, формула (10)). Это и доказывает наши утверждения.

В обозначениях предложения 1 говорят, что последовательность (e_n) получена из последовательности (x_n) с помощью *процесса ортогонализации Грама — Шмидта.*

Предложение 2. *Пусть* Φ *— эрмитова форма на модуле* E *и* (e_i) $(i = 1, \ldots, n)$ *— ортогональный* (соответственно *ортонормальный*) *базис модуля* E. *Тогда для всякого* $p \geqslant 0$ *базис модуля* $\overset{p}{\otimes} E$, *составленный из элементов* $e_{i_1} \otimes \ldots \otimes e_{i_p}$, *и базис* (e_H) *модуля* $\overset{p}{\bigwedge} E$ (*где* H *пробегает множество всех подмножеств из* p *элементов отрезка* $[1, n]$) (см. гл. III, § 5, n° 6) *являются ортогональными* (соответственно *ортонормальными*) *базисами относительно продолжений формы* Φ *на модули* $\overset{p}{\otimes} E$ *и* $\overset{p}{\bigwedge} E$ *соответственно* (§ 1, n° 9). *Если, кроме того, отображения, ассоциированные с формой* Φ, *биективны, то базис* (e'_i) *модуля* E^*, *сопряженный к* (e_i), *ортогонален* (соответственно *ортонормален*) *относительно обратной формы* $\check{\Phi}$ *для формы* Φ (§ 1, n° 7).

Утверждения о модулях $\overset{p}{\otimes} E$ и $\overset{p}{\bigwedge} E$ немедленно следуют из формул (35) и (37) § 1, n° 9, а утверждение относительно обратной формы следует из того, что матрица формы $\hat{\Phi}$ относительно базиса (e'_i) обратна к матрице формы Φ относительно базиса (e_i) (§ 1, n° 10).

2. *Унитарная группа и ортогональная группа*

Пусть Φ — эрмитова форма на модуле E. Автоморфизмы A-модуля E, оставляющие форму Φ инвариантной, называются *унитарными автоморфизмами* (или *унитарными преобразованиями*) относительно формы Φ. Группа этих автоморфизмов называется *унитарной группой, ассоциированной с формой* Φ, и обозначается $\boldsymbol{U}(\Phi)$. Если на модуле E задана квадратичная форма $Q \neq 0$, то автоморфизмы A-модуля E, оставляющие форму Q инвариантной, называются *ортогональными автоморфизмами* (или *ортогональными преобразованиями*) относительно формы Φ. Группа этих автоморфизмов называется *ортогональной группой, ассоциированной с формой* Φ, и обозначается $\boldsymbol{O}(Q)$.

Всякое преобразование, ортогональное относительно некоторой квадратичной формы Q, унитарно относительно билинейной формы, ассоциированной с Q. Обратное верно, если скаляр 2 не равен нулю и не является делителем нуля*) в кольце A (§ 3, n° 4, (13)), например, если A — тело характеристики $\neq 2$.

Рассмотрим, в частности, на модуле $E = A^n$ эрмитову форму Φ_0, матрица которой относительно канонического базиса (e_i) модуля E равна единичной матрице I_n. Унитарные автоморфизмы относительно формы Φ_0 называются просто *унитарными автоморфизмами* (или *унитарными преобразованиями*) *от n переменных*. Группа этих автоморфизмов называется *унитарной группой от n переменных* и обозначается иногда $\boldsymbol{U}(n, A)$ или $\boldsymbol{U}_n(A)$. Матрица U унитарного автоморфизма относительно базиса (e_i) называется *унитарной*. Всякая унитарная матрица обратима и, по формуле (48) § 1, n° 10, удовлетворяет соотношению

$$ {}^tU \cdot U = I_n. \tag{4}$$

*) Слова «не равен нулю» здесь лишние, так как 0 является делителем нуля (гл. I, § 8, n° 3). (*Прим. перев.*)

Обратно, если A — коммутативное кольцо или тело, то всякая матрица, удовлетворяющая условию (4), обратима и унитарна.

Если J — тождественный автоморфизм и 2 не равно 0 *) и не является делителем нуля в кольце A, то вместо предыдущих терминов используются такие: *ортогональная группа от n переменных*, *ортогональный автоморфизм* (или *ортогональное преобразование*) *от n переменных*, *ортогональная матрица*, и вместо $\boldsymbol{U}(n, A)$ (соответственно $\boldsymbol{U}_n(A)$) пишут $\boldsymbol{O}(n, A)$ (соответственно $\boldsymbol{O}_n(A)$). Тогда соотношение (4) принимает вид

$$ {}^tU \cdot U = I_n, \tag{5}$$

и поскольку A коммутативно, это соотношение необходимо и достаточно для того, чтобы матрица U была ортогональной.

Предложение 3. *Пусть A — поле, E — векторное пространство конечной размерности >0, Φ — невырожденная эрмитова форма на пространстве E. Отображение $u \to \det u$ является гомоморфизмом унитарной группы $\boldsymbol{U}(\Phi)$, ассоциированной с Φ, на мультипликативную подгруппу H кольца A, состоящую из элементов ϱ таких, что $\varrho\bar{\varrho} = 1$ (если J — тождественный автоморфизм, то эта подгруппа сводится к $\{-1, 1\}$).*

В самом деле, пусть u — элемент группы $\boldsymbol{U}(\Phi)$, U — его матрица относительно некоторого базиса пространства E, и R — матрица формы Φ относительно этого базиса. Поскольку R обратима, из равенства $R = {}^tURU$ (§ 1, n° 10, формула (48)) следует, что $(\det U)(\det \bar{U}) = 1$. Отсюда $(\det u)\overline{(\det u)} = 1$. Гомоморфизм $u \to \det u$ отображает $\boldsymbol{U}(\Phi)$ на H: в самом деле, если характеристика поля A равна 2, а J — тождественный автоморфизм, то H сводится к 1; в противоположном случае E имеет ортогональный базис (e_i) $(i = 1, \ldots, n)$ (теорема 1); тогда для всякого $\rho \in A$ такого, что $\varrho\bar{\varrho} = 1$, определим автоморфизм u пространства E: $u(e_1) = \varrho e_1$ и $u(e_i) = e_i$ для $i = 2, \ldots, n$; тогда автоморфизм u — унитарный и $\det u = \varrho$, откуда и следует доказываемое утверждение.

В условиях предложения 3 ядро гомоморфизма $u \to \det u$ является нормальной подгруппой в $\boldsymbol{U}(\Phi)$, и называется *специальной унитарной группой*, ассоциированной с формой Φ. Иногда она обозначается символом $\boldsymbol{SU}(\Phi)$.

*) См. предыдущее примечание.

Если J — тождественный автоморфизм и поле A имеет характеристику $\neq 2$, эта группа называется также *специальной ортогональной группой*, ассоциированной с формой Φ (или с квадратичной формой $Q(x) = \Phi(x, x)$) и обозначается $\boldsymbol{SO}(Q)$.

Если $E = A^n$ и матрица формы Φ относительно канонического базиса пространства E единичная, то используются обозначения $\boldsymbol{SU}(n, A)$ или $\boldsymbol{SU}_n(A)$ и $\boldsymbol{SO}(n, A)$ или $\boldsymbol{SO}_n(A)$.

3. *Ортогональные проектирования и инволюции*

В этом n° предполагается, что скаляр 2 *обратим* в кольце A (например, если A — тело характеристики $\neq 2$) и что Φ — *невырожденная* эрмитова форма на модуле E. Обратный элемент к 2 обозначается $\frac{1}{2}$.

Лемма 2. *Для того чтобы эндоморфизм u пространства E удовлетворял условию $u^2 = 1$, необходимо и достаточно, чтобы эндоморфизм $\frac{1}{2}(1 - u)$ был проектированием. Тогда u является разностью двух проектирований: $\frac{1}{2}(1 + u)$ и $\frac{1}{2}(1 - u)$.*

В самом деле, соотношение $\left(\frac{1}{2}(1 - u)\right)^2 = \frac{1}{2}(1 - u)$ в кольце $\mathscr{L}(E)$ равносильно тождеству $u^2 = 1$. Второе утверждение тривиально.

Эндоморфизм u пространства E, удовлетворяющий условию $u^2 = 1$, называется *инволюцией* (эндоморфизм u обязательно является автоморфизмом и совпадает со своим обратным). Положим $v = \frac{1}{2}(1 - u)$, $U^{-1} = v(E)$, $U^+ = v^{-1}(0)$ $(= w(E)$, где $w = \frac{1}{2}(1 + u))$; известно, что E является *прямой суммой* U^+ и U^- (гл. VIII, § 1, n° 1), причем $u(x) = x$ для $x \in U^+$, $u(x) = -x$ для $x \in U^-$. В случае, когда A — тело характеристики $\neq 2$, а пространство E конечномерно, отсюда следует, что все ненулевые собственные векторы автоморфизма u входят либо в U^+, либо в U^-; их собственные значения равны соответственно $+1$ и -1.

Предложение 4. *Пусть $u \in \boldsymbol{GL}(E)$ — инволюция. Следующие свойства эквивалентны:*

а) *эндоморфизм u принадлежит унитарной группе, ассоциированной с Φ;*

б) *подмодули*

$$U^+ = \frac{1}{2}(1 + u)(E) \quad \text{и} \quad U^- = \frac{1}{2}(1 - u)(E)$$

ортогональны (u, *следовательно, неизотропны*).

Кроме того, если A — *тело и* E *конечномерно, то свойства* а) *и* б) *эквивалентны свойству*

в) $u = u^*$.

В самом деле, при $x \in U^+$ и $y \in U^-$ из соотношения $\Phi(u(x), u(y)) = \Phi(x, y)$ следует $2\Phi(x, y) = 0$, то есть а) влечет б). Обратно, равенство $\Phi(u(x), u(y)) = \Phi(x, y)$ выполняется как в случаях, когда элементы x и y оба лежат в U^+ или в U^-, так и, в силу свойства б), в случае, когда один из них лежит в U^+, а другой в U^-; поскольку E является прямой суммой U^+ и U^-, то свойство б) влечет а). Если, наконец, E — конечномерное векторное пространство, то сопряженный эндоморфизм u^* определен, так как форма Φ невырождена; но условие а) равносильно условию $uu^* = 1$ (§ 1, n° 8, следствие предложения 8); по предположению, $u^2 = 1$, то есть свойства а) и в) эквивалентны.

Следствие 1. *Пусть* A — *тело и пространство* E *конечномерно. Отображение* $u \to \frac{1}{2}(1 + u)(E)$ *является биекцией множества инволюций, принадлежащих унитарной группе, ассоциированной с* Φ, *на множество неизотропных подпространств пространства* E; *подпространство* U^+, *соответствующее при этом инволюции* u, *является множеством элементов пространства* E, *инвариантных относительно* u.

В силу предложения 4 достаточно доказать, что всякое неизотропное подпространство M пространства E является множеством инвариантных векторов относительно некоторой единственной инволюции $u \in U(\Phi)$. Но E является прямой суммой подпространств M и M^0 (§ 4, n° 1, следствие предложения 1), и, по предложению 4, должны выполняться равенства $u(x) = x$ для $x \in M$ и $u(x) = -x$ для $x \in M^0$. Эти условия однозначно определяют эндоморфизм u, который, очевидно, и будет удовлетворять требуемым условиям (предложение 4).

Инволюция u, определенная таким образом, называется *симметрией относительно неизотропного подпространства* M.

Следствие 2. *Пусть A — тело, пространство E конечномерно, v — некоторое проектирование пространства E. Для того чтобы подпространства $v(E)$ и $v^{-1}(0)$ были ортогональны (u, следовательно, неизотропны), необходимо и достаточно, чтобы $v = v^*$.*

Достаточно применить к инволюции $u = 1 - 2v$ предложение 4.

Проектирование, удовлетворяющее условию следствия 2, называется *ортогональным проектированием* относительно формы Ф.

4. *Симметрии в ортогональной группе*

В этом n°, если не оговорено противное, предполагается, что *A — поле характеристики $\neq 2$* и Ф — симметрическая билинейная форма, ассоциированная с *невырожденной квадратичной формой Q* на пространстве E. Напомним, что $\Phi(x, x) = 2Q(x)$ для любого $x \in E$ (§ 3, n° 4).

Пусть H — неизотропная гиперплоскость в пространстве E и *u — симметрия относительно H* (n° 3), и пусть вектор $a \neq 0$ ортогонален к H; по предположению, $u(a) = -a$. Всякий вектор $x \in E$ однозначно записывается в виде $x = \lambda a + y$, где $\lambda \in A$ и $y \in H$, но a и y ортогональны, так что $\Phi(x, a) = \lambda\Phi(a, a)$, откуда, поскольку вектор a неизотропный (§ 4, n° 1, следствие предложения 1), $\lambda = \Phi(x, a)\,\Phi(a, a)^{-1}$. Тогда

$$u(x) = \lambda u(a) + u(y) = -\lambda a + y = x - 2\lambda a,$$

откуда

$$u(x) = x - 2\Phi(x, a)\,\Phi(a, a)^{-1}a = x - \Phi(x, a)\,Q(a)^{-1}a. \qquad (6)$$

Заметим, что последний член в равенстве (6) имеет смысл и в случае, если поле A имеет характеристику 2, а вектор *a не сингулярный*; легко проверить, что в этом случае $Q(u(x)) = Q(x)$ для любого $x \in E$, то есть $u \in \boldsymbol{O}(Q)$. Определенная таким образом инволюция u называется также *симметрией* относительно гиперплоскости, ортогональной к вектору a (см. упражнение 28).

Предложение 5. *Пусть векторное пространство E имеет конечную размерность n. Тогда ортогональная группа $\boldsymbol{O}(Q)$, ассоциированная с формой Q, порождается симметриями относительно неизотропных гиперплоскостей пространства E.*

Это утверждение очевидно при $n = 0$, и мы проведем индукцию по числу n. Пусть u — ортогональное преобразование

пространства E, x — неизотропный вектор из E (лемма 1); будем различать три случая:

а) Предположим сначала, что $u(x) = x$. Тогда ортогональная к вектору x гиперплоскость H неизотропна и $u(H) = H$. Поэтому сужение u' преобразования u на эту гиперплоскость принадлежит ортогональной группе $\boldsymbol{O}(Q')$, ассоциированной с сужением Q' формы Q на H. Поскольку форма Q' не вырождена, то, по предположению индукции, $u' = v'_1 \ldots v'_m$, где v'_i — симметрия относительно гиперплоскости L_i в пространстве H. Эндоморфизм v_i пространства E, являющийся продолжением v'_i и удовлетворяющий условию $v_i(x) = x$, будет тогда симметрией относительно гиперплоскости $Ax + L_i$ пространства E. Очевидно, $u = v_1 v_2 \ldots v_m$.

б) Предположим теперь, что $u(x) = -x$. Обозначив через s симметрию относительно гиперплоскости H, ортогональной к вектору x, и положив $v = su$, получим $v(x) = x$ и возвращаемся к случаю а).

в) Переходя к общему случаю, положим $y = u(x)$, откуда $Q(y) = Q(x)$. Векторы $x - y$ и $x + y$ не могут быть *одновременно* изотропными: если $Q(x - y) = 0$ и $Q(x + y) = 0$, то, сложив эти равенства почленно, мы получили бы $2(Q(x) + Q(y)) = 0$ (§ 3, n° 4, определение 2), откуда $4Q(x) = 0$, что противоречит предположению. Предположим, например, что вектор $a = x - y$ неизотропный, тогда

$$\Phi(y, a) = Q(y + a) - Q(y) - Q(a) = Q(x) - Q(y) - Q(a) = -Q(a),$$

и следовательно, обозначая через s симметрию относительно гиперплоскости, ортогональной к вектору a, из формулы (6) будем иметь $s(y) = y + a = x$; положив теперь $v = su$, получим $v(x) = x$ и снова возвращаемся к случаю а). Если $a = x - y$ — изотропный вектор, а $x + y$ — неизотропный, то доказательство, аналогично предыдущему, сводится к случаю б).

5. Группа подобий

Пусть Φ — эрмитова форма на модуле E. Автоморфизм u A-модуля E называется *подобием* (относительно формы Φ), если существует обратимый элемент α кольца A такой, что

$$\Phi(u(x), u(y)) = \alpha\Phi(x, y) \tag{7}$$

для любых $x, y \in E$. Подобия образуют *группу* Γ.

Если форма Ф принимает значения, являющиеся регулярными элементами в кольце A (например, если A — тело и $\Phi \neq 0$), то элемент α в тождестве (7) однозначно определяется автоморфизмом u; этот элемент называется *коэффициентом* подобия u. Подставив λx вместо x в формулу (7), можно убедиться, что α лежит в *центре* кольца A; поменяв в этой формуле местами x и y, получим, кроме того, что $\bar{\alpha} = \alpha$. Если коэффициент подобия автоморфизма u обозначить через $\alpha(u)$, то отображение $u \to \alpha(u)$ будет гомоморфизмом группы Γ в мультипликативную группу обратимых элементов центра кольца A. Ядром этого гомоморфизма является унитарная группа, ассоциированная с формой Ф; следовательно, она нормальная подгруппа в Γ. Пусть β — обратимый элемент центра кольца A, v — гомотетия, соответствующая элементу β, и w — унитарный автоморфизм модуля E, тогда автоморфизм $vw = wv$ является подобием и его коэффициент равен $\beta\bar{\beta}$. Обратно, пусть u — подобие с коэффициентом, имеющим вид $\beta\bar{\beta}$ (где β — обратимый элемент из центра кольца A). Тогда uv^{-1} будет унитарным автоморфизмом w, так что автоморфизм u имеет вид vw.

Предположим теперь, что A — тело, векторное пространство E конечномерно, а форма Ф невырождена. Тогда для всякого подобия u с коэффициентом α выполняются равенства

$$\Phi(x, ay) = a\Phi(x, y) = \Phi(u(x), u(y)) = \Phi(x, u^*(u(y))),$$

то есть u^*u является гомотетией, соответствующей элементу α. Если A коммутативно, n — размерность пространства E, то из формулы (50) § 1, n° 10, следует равенство

$$(\det u)\,\overline{(\det u)} = \alpha^n. \tag{8}$$

Рассмотрим два случая:

1° Число n — *нечетное*, $n = 2q + 1$. Положив $\varrho = \alpha^{-q}(\det u)$, будем иметь $\alpha = (\det u)\,\overline{(\det u)}\,\alpha^{-2q} = \varrho\bar{\varrho}$. Следовательно, подобие u является произведением гомотетии, соответствующей элементу ϱ, и некоторого унитарного автоморфизма.

2° Число n — *четное*, $n = 2q$. Положив $\varrho = \alpha^{-q}(\det u)$, будем иметь $\varrho\bar{\varrho} = 1$. В частности, если J — тождественный автоморфизм, то $(\det u)^2 = \alpha(u)^{2q}$; подобия u, удовлетворяющие условию $\det u = \alpha(u)^q$ (соответственно $\det u = -\alpha(u)^q$), называются *прямыми* (соответственно *обратными*); прямые подобия образуют

в группе Γ подгруппу индекса 2; гомотетии, соответствующие ненулевым элементам, являются прямыми подобиями; ортогональные преобразования с определителем 1 также будут прямыми подобиями; ортогональные преобразования с определителем —1 являются обратными подобиями.

Предыдущие определения и результаты остаются верными и для ε-эрмитовых (§ 3, n° 1), в частности для знакопеременных, форм.

Пусть A — поле и Q — ненулевая *квадратичная форма* на пространстве E. *Подобием* (относительно формы Q) называется автоморфизм u пространства E, для которого существует ненулевой элемент $\alpha \in A$ (называемый *коэффициентом подобия*) такой, что $Q(u(x)) = \alpha Q(x)$ для любого $x \in E$. Ясно, что в этом случае автоморфизм u будет подобием с коэффициентом α относительно билинейной формы, ассоциированной с формой Q; обратное верно, если характеристика поля A отлична от 2.

6. *Эрмитова геометрия*

Определение 2. *Пусть A — тело, L — аффинное пространство над A, и T — пространство переносов L* (гл. II, приложение II). *Если на пространстве T определена невырожденная эрмитова форма Φ, то L называется эрмитовым пространством над телом A, а Φ — метрической формой пространства L.*

Если J — тождественный автоморфизм (и, значит, A коммутативно), то L чаще называется *евклидовым пространством*.

Для любых двух точек a и b пространства L положим $e(a, b) = \Phi(b - a, b - a)$. Пусть c — некоторая третья точка L. Для того чтобы векторы $b - a$ и $c - a$ были ортогональны, необходимо, чтобы $e(b, c) = e(a, b) + e(a, c)$ (§ 1, n° 5, формула (17)). Если $J = 1$ и характеристика поля A не равна 2, то это условие достаточно («теорема Пифагора»).

Два линейных многообразия пространства L называются *ортогональными*, если их направляющие подпространства (гл. II, приложение II, n° 3) ортогональны. Линейное многообразие в L называется изотропным (соответственно вполне изотропным), если его направляющее подпространство изотропно (соответственно вполне изотропно). Вектор пространства T называется ортогональным к линейному многообразию пространства L, если он ортогонален к его направляющему подпространству.

Пусть V — линейное многообразие в пространстве L, и x — точка L. Множество точек $y \in L$ таких, что вектор $y - x$ ортогонален к L, является линейным многообразием, проходящим через точку x. Многообразие W называют *полным ортогональным* (или просто *ортогональным*) многообразием к V, проходящим через точку x. Если пространство L конечномерно, то размерность W равна коразмерности V. Кроме того, если V неизотропно, то направляющие подпространства многообразий V и W являются дополнениями друг друга (§ 4, n° 1, следствие предложения 1); тогда W и V пересекаются в единственной точке x_1; легко видеть, что если взять начало в многообразии V, V фиксировано, то отображение $x \to x_1$ будет идемпотентным аффинным линейным отображением; это отображение называется ортогональной проекцией пространства L на многообразие V; линейное отображение, ассоциированное с ним (гл. II, приложение II, n° 4), будет ортогональным проектированием пространства T на направляющее подпространство многообразия V (n° 3).

Определение 3. *Пусть L — эрмитово пространство над телом A, T — пространство переносов пространства L. Аффинная биекция и пространства L на L называется перемещением* (соответственно *подобием*) *пространства L, если ассоциированное с ней линейное отображение v пространства T в T* (гл. II, приложение II, n° 4) *унитарно* (соответственно *является подобием*).

Группа переносов является нормальной подгруппой аффинной группы и поэтому будет нормальной подгруппой в группе подобий и в группе движений. Пусть G_a ($a \in L$) — группа подобий (соответственно перемещений), оставляющих точку a неподвижной. Если отождествить L с T, приняв a за начало координат, то G_a будет группой подобий (соответственно унитарной группой) пространства T. Всякое подобие (соответственно перемещение) u может быть единственным образом представлено в виде $u = u_1 t_1$, где $u_1 \in G_a$ и $t_1 \in T$, а также в виде $u = t_2 u_2$, где $u_2 \in G_a$ и $t_2 \in T$; впрочем, $u_2 = u_1$ и $t_2 = u_1 t_1 u_1^{-1}$ (гл. II, приложение II, n° 4).

Пусть u — подобие в пространстве L, v — ассоциированное с ним подобие в T. Коэффициент подобия преобразования v называется также коэффициентом подобия преобразования u (n° 5). Обозначим коэффициент подобия преобразования u симво-

лом $\alpha(u)$, тогда отображение $\alpha \to \alpha(u)$ является гомоморфизмом группы подобий пространства L в мультипликативную группу обратимых элементов кольца A; его ядром является группа перемещений, которая, следовательно, меньше всей группы подобий. В случае, когда тело A коммутативно и пространство L конечномерно, определитель $\det u$ (равный, по определению, $\det v$) и коэффициент $\alpha(u)$ связаны теми же соотношениями, что и в n° 5. Движения u, у которых $\det u = 1$, образуют в группе перемещений нормальную подгруппу. Эта подгруппа имеет индекс 2, если характеристика поля $A \neq 2$, а J — тождественный автоморфизм.

Предложение 6. *Пусть E — конечномерное эрмитово пространство над телом A и индекс его метрической формы равен нулю. Тогда всякое подобие и пространства L с коэффициентом $\mu \neq 1$ имеет единственную неподвижную точку.*

В самом деле, пусть a — точка пространства L. Существуют подобие v пространства L, оставляющее точку a неподвижной, и перенос t пространства L такой, что $u = tv$. Точка b остается неподвижной при подобии u в том и только в том случае, когда $v(b) - b = t$. Чтобы показать, что это уравнение имеет единственное решение, отождествим L с его пространством переносов T, приняв точку a за начало. Теперь достаточно доказать, что эндоморфизм $v - 1$ пространства T обратим, то есть равенство $v(x) - x = 0$ $(x \in T)$ влечет $x = 0$. Но если $v(x) - x = 0$, то $\Phi(x, x) = \Phi(v(x), v(x)) = \mu\Phi(x, x)$, откуда $\Phi(x, x) = 0$, поскольку $\mu \neq 1$. Но тогда $x = 0$, так как индекс формы Φ равен нулю, что и требовалось доказать.

Предположим, что A — тело характеристики $\neq 2$. Всякое движение u пространства L такое, что $u^2 = 1$, имеет по крайней мере одну неподвижную точку, например середину $\frac{1}{2}(x + u(x))$ отрезка, соединяющего две соответствующие точки. Приняв эту точку за начало, мы обнаружим, что унитарный автоморфизм пространства T, ассоциированный с движением u, является симметрией (n° 3). Пусть V — неизотропное линейное многообразие в L; движение u называется *симметрией относительно V*, если, взяв начало координат в V, это движение можно отождествить с симметрией пространства T относительно V. Это озна-

чает, что $u(x)$ получается следующим способом: пусть x_1 — ортогональная проекция вектора x на многообразие V, тогда $u(x) - x = 2(x_1 - x)$.

У п р а ж н е н и я. 1) Пусть A — поле и R — эрмитова матрица порядка n над полем A. *Главными минорами* порядка r матрицы R называются миноры, получаемые вычеркиванием из A $n - r$ строк и $n - r$ столбцов с одинаковыми номерами.

а) Показать, что если в матрице R некоторый главный минор порядка r отличен от нуля, а все содержащие его миноры порядков $r + 1$ и $r + 2$ равны нулю, то ранг матрицы R равен r (см. гл. III, § 7, упражнение 1 и § 8, упражнение 11 и гл. IV, § 2, упражнение 10). Вывести отсюда, что ранг матрицы R равен r тогда и только тогда, когда в ней существует главный минор порядка r, отличный от нуля, а все главные миноры порядков $r + 1$ и $r + 2$ равны нулю.

б) Пусть ранг матрицы R равен r. Показать, что существует перестановка $\sigma \in \mathfrak{S}_n$ такая, что после применения ее *одновременно* к строкам и столбцам матрицы R главные миноры Δ_k порядка k новой матрицы S, полученные из нее вычеркиванием строк и столбцов с номерами $> k$, удовлетворяют условиям: $1°\ \Delta_r \neq 0$; $2°$ ни для какого $k < r$ не выполняются равенства $\Delta_k = \Delta_{k+1} = 0$.

2) Пусть A — поле, E — пространство конечной размерности n, Φ — эрмитова полуторалинейная форма на E, удовлетворяющая условию (Т) § 4, n° 2, $R = (a_{ij})$ — матрица формы Φ относительно некоторого базиса (e_i) пространства E.

а) Пусть ранг формы Φ равен r и главный минор (упражнение 1), полученный из R вычеркиванием строк и столбцов с номерами $> r$, отличен от нуля. Показать, что в пространстве E найдется новый базис (f_i) такой, что $e_i = f_i$ при $1 \leqslant i \leqslant r$. При этом матрица формы Φ относительно этого базиса получается из R подстановкой нуля вместо всех элементов α_{ij} с индексами $i > r$ или $j > r$ (рассмотреть подпространство E^0, ортогональное к E).

б) Пусть форма Φ имеет ранг n и алгебраическое дополнение Δ_{n-1} элемента α_{nn} в определителе $\Delta = \det R$ отлично от нуля. Вывести из а), что в пространстве E существует новый базис (f_i) такой, что $f_i = e_i$, $1 \leqslant i \leqslant n - 1$, и

$$\Phi(x, y) = \Phi\Big(\sum_{i=1}^{n} \xi_i f_i, \sum_{i=1}^{n} \eta_i f_i\Big) = \sum_{i=1}^{n-1}\sum_{j=1}^{n-1} \alpha_{ij}\xi_i\bar{\eta}_i + \frac{\Delta}{\Delta_{n-1}}\xi_n\bar{\eta}_n$$

(рассмотреть эрмитову форму, матрица которой относительно базиса (e_i) получается из R заменой элемента α_{nn} на $\alpha_{nn} - \frac{\Delta}{\Delta_{n-1}}$).

в) Пусть ранг формы Φ равен n, $\Delta_{n-1} = 0$, но минор Δ_{n-2}, полученный из R вычеркиванием строк и столбцов с номерами $n - 1$ и n,

отличен от нуля. Показать, что в пространстве E найдется новый базис (f_i) такой, что $f_i = e_i$, $1 \leqslant i \leqslant n-2$, и

$$\Phi(x, y) = \Big(\sum_{i=1}^{n} \xi_i f_i, \sum_{i=1}^{n} \eta_i f_i\Big) = \sum_{i=1}^{n-2}\sum_{i=1}^{n-2} \alpha_{ij}\xi_i\bar{\eta}_j + \xi_{n-1}\bar{\eta}_n + \xi_n\bar{\eta}_{n-1}.$$

(Пусть H — изотропная гиперплоскость, порожденная элементами $e_1, \ldots, e_{n-1}$; заметить, что прямая, ортогональная к H, не содержится в подпространстве, порожденном элементами $e_1, \ldots, e_{n-1}$; применить предложение 2 § 4, n° 2.)

3) Пусть A — конечное поле, E — векторное пространство конечной размерности над полем A, Φ — невырожденная эрмитова форма на E, полуторалинейная относительно автоморфизма $J \neq 1$ поля A. Показать, что пространство E обладает ортонормальным относительно формы Φ базисом (см. гл. V, § 11, n° 5, следствие теоремы 3).

4) Пусть A — конечное поле характеристики $\neq 2$, E — векторное пространство конечной размерности n над полем A.

а) Показать, что для любой невырожденной симметрической билинейной формы на пространстве E существует ортогональный базис (e_i) этого пространства такой, что $\Phi(e_i, e_i) = 1$ при $1 \leqslant i \leqslant n-1$, $\Phi(e_n, e_n) = \Delta$ (дискриминант формы Φ относительно базиса (e_i)). (Заметить, что при $\alpha\beta \neq 0$ уравнение $\alpha\xi^2 + \beta\eta^2 = \gamma$, где $\gamma \neq 0$, всегда имеет решения (ξ, η) в поле A (гл. V, § 11, упражнение 4).)

б) Для того чтобы две невырожденные билинейные симметрические формы на E были эквивалентны, необходимо и достаточно, чтобы отношение их дискриминантов (относительно одного и того же базиса) было в поле A квадратом. Вывести отсюда, что при нечетном n для всякой невырожденной симметрической билинейной формы Φ в пространстве E существует ортогональный базис, относительно которого матрица формы Φ имеет вид λI_n $(\lambda \in A)$, следовательно, индекс формы Φ равен $(n-1)/2$.

в) Показать, что при n четном, $n = 2m$, индекс невырожденной симметрической билинейной формы Φ на пространстве E равен m, если элемент $(-1)^m \Delta$ является квадратом в поле A, и равен $m-1$ в противоположном случае.

5) Пусть A — поле характеристики $\neq 2$ и I — многочлен от $n(n+1)/2$ переменных X_{ij} $(1 \leqslant i \leqslant j \leqslant n)$ с коэффициентами из A; для всякой *симметрической* матрицы $R = (\alpha_{ij})$ с элементами из некоторого надполя A' поля A через $I(R)$ обозначим элемент поля A', получаемый из многочлена I подстановкой элементов αij вместо переменных X_{ij} $(i \leqslant j)$.

Предположим, что многочлен I обладает следующим свойством:

$$I({}^tPUP) = (\det P)^h I(U),$$

где матрица $U = (u_{ij})$, $u_{ij} = X_{ij}$ при $i \leqslant j$, $u_{ij} = X_{ij}$ при $i > j$, $P = (Y_{ij})$ — квадратная матрица порядка n (Y_{ij} — еще один набор

n^2 переменных), $h > 0$ — целое число. Показать, что h *четно*, $h = 2k$, $I(U) = \gamma (\det U)^k$, где $\gamma \in A$. (Применяя теорему 1, показать, что для всякой симметрической матрицы R над алгебраическим замыканием Ω поля A выполняется равенство $(I(R))^2 = \lambda (\det R)^h$, где $\lambda \in \Omega$; рассматривая в многочлене $\det U$ от переменных X_{ij} слагаемые, содержащие некоторое X_{ii}, воспользоваться тем, что этот многочлен не является квадратом.)

° 6) Пусть A — полное не дискретное нормированное поле характеристики $\neq 2$ (Общ. топол., гл. IX, § 3, n° 2), Φ — невырожденная эрмитова форма на векторном пространстве E конечной размерности n над полем A, $R = (\alpha_{ij})$ — матрица формы Φ относительно базиса (e_i) пространства E. Показать, что существует такое $\varepsilon > 0$, что для всякой матрицы $R' = (\alpha'_{ij})$, удовлетворяющей условиям $|\alpha'_{ij} - \alpha_{ij}| \leqslant \varepsilon$ для всех пар (i, j), форма Φ', имеющая относительно базиса (e_i) матрицу R, эквивалентна форме Φ. (Свести доказательство к случаю, когда матрица R диагональна; воспользоваться упражнением 2б), опираясь на следующую лемму: существует такое число $a > 0$, что при $|\eta| \leqslant a$ найдется элемент $\xi \in A$, удовлетворяющий равенству $\xi^2 = 1 - \eta$. Для доказательства этой леммы использовать разложение в ряд бинома $(1 - x)^{1/2}$.)

*7) Пусть A — *неупорядочиваемое* поле (гл. VI, § 2, упражнение 8) характеристики $\neq 2$, E — векторное пространство конечной размерности $n > 0$ над полем A, Q — невырожденная квадратичная форма на пространстве E, (e_i) — базис, ортогональный относительно Q. Тогда $Q\left(\sum_{i=1}^{n} \xi_i e_i\right) = \sum_{i=1}^{n} \alpha_i \xi_i^2$. Положим $Q_r(\xi_1, \ldots, \xi_r) = \sum_{i=1}^{r} \alpha_i \xi_i^2$, $1 \leqslant r \leqslant n$, и через M_r обозначим множество значений функции Q_r, когда скаляры ξ_i $(1 \leqslant i \leqslant r)$ пробегают поле A.

а) Предположим, что для некоторого номера r выполняется равенство $M_r = M_{r+1}$; показать, что $M_r = A$ (заметить, что всякий элемент поля A является суммой квадратов (гл. VI, § 2, упражнение 7)).

б) Предположим, что подгруппа S, состоящая из квадратов элементов поля A, имеет в мультипликативной группе A^* *конечный* индекс s. Вывести из а), что при $n > s$ всякая невырожденная квадратичная форма на пространстве E имеет индекс > 0 (заметить, что каждое множество M_r является объединением нуля и некоторых классов по mod S). Рассмотреть применение к случаю, когда A — поле p-адических чисел $\mathbf{Q}_p$ (Общ. топол., гл. III, § 5, упражнение 35).

8) Пусть A — поле характеристики $\neq 2$, E — конечномерное векторное пространство размерности n над полем A, Q — невырожденная квадратичная форма индекса 0 на пространстве E. Пусть

A' — алгебраическое расширение конечной *нечетной* степени поля A, E' — векторное пространство над полем A', полученное из E расширением поля скаляров до A'. Показать, что продолжение Q' формы Q на пространство E' (§ 3, n° 4, предложение 3) также имеет индекс 0. (Свести доказательство к случаю, когда $A' = A[X]/(f)$, где f — неприводимый многочлен над полем A нечетной степени m. Пусть (e_i) — ортогональный относительно формы Q базис пространства E и $\varrho_i = Q(e_i)$; показать, что в кольце $A[X]$ не может быть выполнено соотношение $\sum_i \varrho_i (g_i(x))^2 = f(X)\, h(X)$, где все g_i — отличные от нуля многочлены степени $\leqslant m - 1$; для этого заметить, что многочлен h непременно должен иметь нечетную степень, и рассмотреть какой-нибудь его неприводимый множитель нечетной степени.)

9) Пусть A — тело, E — векторное пространство над A со счетным базисом $(e_n)_{n \geqslant 1}$, Φ — невырожденная эрмитова полуторалинейная форма на E, удовлетворяющая условию (T) (§ 4, n° 2).

а) Показать, что если условие (C) теоремы 1 не выполняются одновременно, то в пространстве E существует базис, ортогональный относительно Φ (рассуждать, как в упражнении 4 § 5).

б) Предположим, что, кроме того, A — поле и существует целое число s такое, что всякая невырожденная эрмитова полуторалинейная форма на любом векторном пространстве конечной размерности $> s$ над полем A имеет индекс > 0 (см. упражнение 7). Показать, что в пространстве E имеется базис, ортонормальный относительно Φ. (Рассуждать, как в а), заметив сначала, что для всякой невырожденной эрмитовой формы Ψ на пространстве F конечной размерности $> s$ и всякого элемента поля A, имеющего вид $\alpha = \lambda + \overline{\lambda}$, найдется вектор $z \in F$ такой, что $\Psi(z, z) = \alpha$ (см. § 4, n° 2, предложение 4).)

*10) а) Пусть A — кольцо главных идеалов, в котором имеется единственный максимальный идеал $A\pi$ такой, что 2 не делится на π (гл. VII, § 1, упражнение 4). Пусть E — свободный A-модуль размерности n. Показать, что всякая симметрическая билинейная форма Φ на модуле E имеет ортогональный базис. (Пусть r — наибольший показатель степени, для которого π^r делит все элементы $\Phi(x, y)$; показать, что существует $a \in E$ такой, что $\Phi(a, a) = \alpha\pi^r$, где α — обратимый элемент кольца A; вывести отсюда, что модуль E является прямой суммой подмодуля $F = Aa$ и подмодуля F^0, ортогонального к F.)

б) Привести пример (для $n = 2$), в котором форма Φ невырождена и в модуле E существует неизотропный подмодуль F ранга 1, обладающий в E дополнением, однако F^0 не является его дополнением.

в) Пусть (e_i) — базис, ортогональный относительно Φ, и $\alpha_i = \Phi(e_i, e_i)$. Показать, что идеалы $A\alpha_i$ с точностью до порядка не зависят от рассматриваемого ортогонального базиса (см. § 5, теорема 1).

Эти идеалы называются *инвариантными множителями* формы Φ. Привести пример двух форм, имеющих одинаковые инвариантные множители и не эквивалентных (взять две формы, у которых отношение дискриминантов не является квадратом).

г) Пусть F — подмодуль в E, Φ_F — ограничения формы Φ на $F \times F$ и инвариантные ненулевые множители $A\alpha_i$ $(1 \leqslant i \leqslant r)$ формы Φ занумерованы таким образом, что α_i делит α_{i+1}; пусть инвариантные множители $A\beta_i$ $(1 \leqslant i \leqslant s)$ формы Φ_F занумерованы таким образом, что β_i делит β_{i+1}. Показать, что $s \leqslant r$ и при $1 \leqslant i \leqslant s$ элемент β_i кратен α_i (так же, как в упражнении 1а) § 5).

д) Пусть форма Φ невырождена; пусть F, G — неизотропные подмодули модуля E такие, что F^0 (соответственно G^0) является дополнением к F (соответственно к G). Предположим, что сужения формы Φ на F и G эквивалентны; показать, что существует автоморфизм модуля E, оставляющий форму Φ инвариантной и такой, что $u(F) = G$. (Пользуясь упражнением а), свести доказательство к случаю, когда $F = Aa$, $G = Ab$, $\Phi(a, a) = \Phi(b, b)$. Пусть (c_j) — некоторый базис модуля G^0, b' и c'_j $(1 \leqslant j \leqslant n-1)$ — компоненты соответственно элементов b и c_j в F^0; показать, что найдутся такие скаляры μ_j $(1 \leqslant j \leqslant n-1)$, что элементы $d_j = c'_j + \mu_j b'$ удовлетворяют соотношениям $\Phi(d_j, d_k) = \Phi(c_j, c_k)$ для любых индексов j и k; для этого заметить, что при любом $\lambda \in A$ один из элементов $1 \pm \lambda$ обратим в кольце A.)

11) Пусть A — кольцо главных идеалов характеристики 0, в котором имеется единственный главный идеал π такой, что 2 делится на π. Пусть Φ — симметрическая билинейная форма на модуле $E = A^2$, определенная формулой $\Phi(\xi_1 e_1 + \xi_2 e_2, \eta_1 e_1 + \eta_2 e_2) = \xi_1\eta_2 + \xi_2\eta_1$, где (e_1, e_2) — канонический базис модуля E. Показать, что модуль E не имеет базиса, ортогонального относительно Φ.

12) Пусть A — конечное поле $\boldsymbol{F}_{q^2}$, J — инволютивный автоморфизм $\xi \to \xi^q$ поля A, инвариантное поле которого есть $\boldsymbol{F}_q$. Пусть, далее, E — векторное пространство размерности n над полем A, Φ — невырожденная эрмитова форма на пространстве E, полуторалинейная относительно J. Показать, что порядок унитарной группы $U(\Phi)$ равен

$$(q^n - (-1)^n)\, q^{n-1}\, (q^{n-1} - (-1)^{n-1})\, q^{n-2} \ldots (q^2 - 1)\, q\, (q+1)$$

(доказательство такое же, как в упражнении 10 § 5; воспользоваться упражнением 3).

13) Пусть A — конечное поле $\boldsymbol{F}_q$ (q не кратно 2), E — векторное пространство размерности n над A, Q — невырожденная квадратичная форма на пространстве E. Показать, что

а) если n нечетно, то порядок группы $\boldsymbol{SO}(Q)$ равен

$$(q^{n-1} - 1)\, q^{n-2}\, (q^{n-3} - 1)\, q^{n-4} \ldots (q^2 - 1)\, q;$$

б) если $n = 2m$ четно, то порядок группы $\boldsymbol{SO}(Q)$ равен
$$(q^{2m-1} - \varepsilon q^{m-1})(q^{2m-2} - 1)\, q^{2m-3} \ldots (q^2 - 1)\, q,$$
где $\varepsilon = 1$, если $(-1)^m \Delta$ является квадратом в поле A, и $\varepsilon = -1$ в противоположном случае, Δ — дискриминант формы Q в произвольном базисе пространства E (доказательство такое же, как и в упражнении 12; использовать упражнение 3 § 6 и упражнение 5 гл. V, § 11).

14) Пусть A — поле, E — векторное пространство над A конечной размерности $n \geqslant 2$, Φ — невырожденная эрмитова полуторалинейная форма на пространстве E, удовлетворяющая условию (T) (§ 4, n° 2). Показать, что единственными эндоморфизмами w пространства E, перестановочными со всеми автоморфизмами u из специальной унитарной группы $\boldsymbol{SU}(\Phi)$, являются гомотетии; исключение представляет лишь случай, когда одновременно выполняются условия $n = 2$, $J = 1$ и характеристика поля $A \neq 2$. (При $n \geqslant 3$ записать, что эндоморфизм w перестановочен с инволюциями $u \in \boldsymbol{SU}(\Phi)$, и применить упражнение 3 § 4; при $n = 2$, $J \neq 1$ записать, что w перестановочен со всеми элементами из $\boldsymbol{SU}(\Phi)$, матрицы которых относительно некоторого ортогонального базиса пространства E имеют вид $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$.)

*15) Пусть A — поле характеристики $\neq 2$, E — векторное пространство над A размерности $n \geqslant 1$, Q — невырожденная квадратичная форма на пространстве E. Для всякого автоморфизма $u \in \boldsymbol{O}(Q)$ положим $w = u - 1$, и пусть r — ранг w, $W = \overset{-1}{w}(0)$.

а) Показать, что $w(E)$ есть подпространство W^0, ортогональное к W.

б) Показать, что при $n = 2$, $r = 2$ автоморфизм u является произведением двух симметрий относительно прямых пространства E. (Установить, что если вектор $w(x)$ изотропен при любом неизотропном векторе $x \in E$, то он изотропен при любом $x \in E$; рассмотреть отдельно случаи, когда поле A имеет не меньше пяти элементов, и случай $A = \boldsymbol{F}_3$.)

в) Пусть n и r — произвольные целые числа. Показать, что если образ $w(E)$ не вполне изотропен, то автоморфизм u является произведением r симметрий относительно гиперплоскостей пространства E и не может быть представлен в виде произведения меньшего числа симметрий. (Свести доказательство к случаю, когда W вполне изотропно, и применить индукцию по n и r. Пользуясь тем, что всякая плоскость, в которой все прямые, кроме, быть может, одной, изотропны, будет непременно вполне изотропной, и рассуждая от противного, доказать, что при $W \neq \{0\}$ существует вектор $a \in W^0$ такой, что вектор $w(a)$ неизотропен; рассмотреть автоморфизм su, где s — симметрия относительно гиперплоскости, ортогональной к $w(a)$;

при $W = \{0\}$ взять вектор $a \in E$ такой, что $w(a)$ неизотропен, снова рассмотреть автоморфизм su, где s — та же симметрия, что и раньше, и воспользоваться упражнением б).)

г) Предположим, что подпространство $w(E)$ вполне изотропно. Пусть s — симметрия относительно неизотропной гиперплоскости H. Показать, что подпространство векторов, инвариантное относительно su, есть $H \cap W$ и имеет, следовательно, размерность $n - r$. Вывести отсюда, что автоморфизм su не может быть представлен в виде произведения менее чем $r + 1$ симметрий относительно гиперплоскостей. Затем вывести из в), что автоморфизм u является произведением $r + 2$ симметрий, но не может быть представлен в виде произведения меньшего числа симметрий.

д) Вывести из в) и г), что всякий ортогональный автоморфизм является произведением не более чем n симметрий относительно гиперплоскостей.

е) Показать, что при n нечетном (соответственно четном) для всякого автоморфизма $u \in \boldsymbol{O}(Q)$ с определителем 1 (соответственно -1) найдется инвариантный относительно u вектор $x \neq 0$ (применить д)).

16) В предположениях упражнения 15 показать, что при $n \geqslant 3$ группа $\boldsymbol{SO}(Q)$ порождается симметриями относительно неизотропных подпространств размерности $n - 2$ (рассуждать, как в предложении 5 § 4).

*17) Предположения те же, что в упражнении 15.

а) Показать, что коммутант $\Omega(Q)$ ортогональной группы $\boldsymbol{O}(Q)$ порождается элементами $(st)^2$, где s и t пробегают множество симметрий относительно гиперплоскостей (применить предложение 5 § 4 и заметить, что в любой группе Г подгруппа, порожденная квадратами элементов Г, содержит коммутант группы Г).

б) Показать, что при $n \geqslant 3$ коммутант группы $\boldsymbol{SO}(Q)$ порождается квадратами элементов $\boldsymbol{SO}(Q)$ (применить упражнение 16); вывести отсюда, что эта группа совпадает с $\Omega(Q)$, а факторгруппа $\boldsymbol{SO}(Q)/\Omega(Q)$ коммутативна и все ее элементы имеют порядок 2.

в) Плоскость $P \subset E$ называется *гиперболической*, если она неизотропна и содержит изотропные прямые (обязательно две). Автоморфизм $u \in \boldsymbol{O}(Q)$ называется *гиперболическим*, если существует гиперболическая плоскость P такая, что $u(x) = x$ для всех $x \in P^0$; автоморфизм u называется тогда гиперболическим преобразованием, ассоциированным с P. Показать, что если индекс формы $Q \geqslant 1$, то всякий автоморфизм $u \in \boldsymbol{O}(Q)$ является произведением гиперболических преобразований (воспользоваться предложением 5 § 4 и упражнением 4а) § 4). Вывести отсюда, что если плоскость P — гиперболическая, то всякий автоморфизм $u \in \boldsymbol{O}(Q)$ может быть записан в виде $u = tv$, где t — гиперболическое преобразование, ассоциированное с P, и $v \in \Omega(Q)$.

*18) Пусть A — поле, E — векторное пространство размерности n над полем A, Φ — невырожденная эрмитова полуторалинейная

форма на пространстве E, удовлетворяющая условию (Т) (§ 4, n° 2). Пусть V — векторное подпространство в E и H_V — подгруппа унитарной группы $\boldsymbol{U}$ (Ф), состоящая из унитарных автоморфизмов u таких, что $U(V) = V$.

а) Показать, что если V не является вполне изотропным подпространством размерности $n/2$, то образ группы H_V при отображении $u \to \det u$ будет в A^* подгруппой, состоящей из элементов $\varrho \in A$, удовлетворяющих условию $\varrho\bar{\varrho} = 1$.

б) Показать, что если (при n четном) V — вполне изотропное подпространство размерности $n/2$, то образ группы H_V при отображении $u \to \det u$ образует в A^* подгруппу, состоящую из элементов вида $\bar{\lambda}/\lambda$ (применить предложение 2 § 4, n° 2).

в) Пусть V, W — векторные подпространства в E и сужения формы Ф на V и W эквивалентны. Показать, что в следующих случаях существует автоморфизм $u \in \boldsymbol{SU}$ (Ф) такой, что $u(V) = W$:

1° $J \neq 1$ (применить теорему 3, гл. V, § 11, n° 5).

2° $J = 1$, характеристика поля $A \neq 2$, V и W не являются вполне изотропными подпространствами размерности $n/2$.

г) Пусть $J = 1$, характеристика поля $A \neq 2$, $n = 2m$ четно, Ф — невырожденная симметрическая билинейная форма индекса m, V и W — вполне изотропные подпространства размерности m; показать, что определитель всякого ортогонального автоморфизма u такого, что $u(V) = W$, равен $\det u = (-1)^{m-q}$, где $q = \dim(V \cap W)$ (использовать б) и предложение 2 § 4, n° 2). Вывести отсюда, что множество вполне изотропных подпространств размерности m является объединением двух классов интранзитивности N_1, N_2 группы $\boldsymbol{SU}$ (Ф); если подпространства V и W лежат в одном классе (соответственно в разных классах), то размерность пересечения $V \cap W$ имеет ту же четность, что и m (соответственно имеет четность другую, чем m). Для того чтобы подобие u (относительно Ф) было прямым, необходимо и достаточно, чтобы выполнялось равенство $u(N_1) = N_1$ (воспользоваться упражнением 4в) § 4).

19) Пусть A — тело, E — векторное пространство над A конечной размерности > 0, Ф — невырожденная и не знакопеременная ε-эрмитова полуторалинейная форма на E. Пусть автоморфизм u пространства E обладает свойством:

$$\Phi(u(x), u(x)) = \alpha\Phi(x, x)$$

для всех $x \in E$, $\alpha \in A$. Показать, что u — подобие с коэффициентом α; исключение представляет лишь случай, когда одновременно A — поле характеристики 2, J — тождественный автоморфизм (использовать упражнение 8 § 1).

20) Пусть A — тело, L — эрмитово пространство конечной размерности над полем A; предположим, что метрическая форма Ф пространства L удовлетворяет условию (Т) (§ 4, n° 2). Показать, что если индекс формы Ф больше 0, то существуют подобия (относитель-

но Ф) пространства L с коэффициентом $\neq 1$, не имеющие неподвижных точек (применить рассуждение из доказательства предложения 6 § 6 и предложение 2 § 4, n° 2).

21) Пусть A — поле характеристики $\neq 2$, L — конечномерное евклидово пространство над полем A, Ф — метрическая форма пространства L.

а) Показать, что всякая биекция u пространства L на себя, удовлетворяющая условиям

$$\Phi(u(x)-u(y),\ u(x)-u(y))=\Phi(x-y,\ x-y)$$

для любых $x, y \in L$, является перемещением (воспользоваться упражнением 7 § 1).

б) Показать, что группа перемещений порождается симметриями относительно неизотропных гиперплоскостей аффинного пространства L (пользуясь предложением 5 § 4, свести к случаю, когда всякий неизотропный сдвиг является произведением двух таких симметрий).

22) Два линейных многообразия эрмитова пространства L называются *перпендикулярными*, если их направляющие подпространства слабо ортогональны (§ 3, упражнение 11). Пусть пространство L конечномерно, V_1, V_2 — линейные многообразия, W_1, W_2 — их направляющие подпространства. Пусть $p = \dim(W_1 + W_2) < n$; показать, что если подпространство $W_1 + W_2$ неизотропно, то существует по крайней мере одно линейное многообразие U размерности $n - p$, перпендикулярное к V_1 и к V_2 и пересекающее каждое из них в единственной точке; кроме того, объединение всех таких линейных многообразий U является линейным многообразием размерности $n - p + q$, где $q = \dim(W_1 \cap W_2)$.

23) Пусть A — поле характеристики $\neq 2$, E — векторное пространство конечной размерности $n + 1 \geqslant 2$ над полем A, Q — квадратичная форма на пространстве E, Ф — ассоциированная с Q симметрическая билинейная форма. Множество C, состоящее из векторов $x \in E$, удовлетворяющих условию $Q(x) = 0$, называется *изотропным конусом* с вершиной 0 и с уравнением $Q(x) = 0$. Если это множество не сводится к 0, то образ S множества $C - \{0\}$ при каноническом отображении π множества $E - \{0\}$ в проективное пространство $\boldsymbol{P}(E)$ (гл. II, приложение III) называется *проективной квадрикой* (соответственно при $n = 2$ *проективной коникой*) однородного уравнения $Q(x) = 0$. Если форма Q невырождена, то и S называется *невырожденной*. Два проективных линейных многообразия V_1, V_2 пространства $\boldsymbol{P}(E)$ называются *сопряженными* относительно S, если прообразы $\overset{-1}{\pi}(V_1)$ и $\overset{-1}{\pi}(V_2)$ ортогональны (относительно Ф). *Полярой* V^0 проективного линейного многообразия $V \subset \boldsymbol{P}(E)$ относительно S называется такое многообразие, что объединение $\overset{-1}{\pi}(V^0) \cup \{0\}$ является подпространством, вполне ортогональным (относительно Ф) к $\overset{-1}{\pi}(V) \cup \{0\}$; если V — гиперплоскость и S невырождена, то V^0 состоит из одной точки, называемой *полюсом* гипер-

плоскости V. Проективное линейное многообразие V называется *касательным* к S, если подпространство $\overline{\pi}^{-1}(V) \cup \{0\}$ изотропно (относительно Ф).

Ниже мы предполагаем, что S непуста и невырождена.

а) Показать, что пересечение квадрики S со всяким проективным линейным многообразием V либо пусто, либо является квадрикой *в многообразии* V; для того чтобы эта квадрика была вырождена, необходимо и достаточно, чтобы многообразие V было касательным к S.

б) Показать, что гиперплоскость, касательная к квадрике S в точке $z \in S$, является объединением прямых, проходящих через точку z и касательных к S.

в) Пусть $z \overline{\in} S$. Для всякой прямой D, проходящей через точку z и пересекающей S в двух точках a, b (различных или нет), обозначим через z' точку, *гармонически сопряженную* к z относительно точек a и b, то есть такую точку прямой D, что $\begin{bmatrix} a & b \\ z' & z \end{bmatrix} = -1$ (гл. II, приложение III, упражнение 4); показать, что точка z' лежит в гиперплоскости, полярной к точке z относительно S; показать также, что существует n таких точек, принадлежащих квадрике S и образующих в $\boldsymbol{P}(E)$ проективно свободное множество (см. § 4, упражнение 4а)).

г) Пусть $n = 3$ и форма Ф имеет максимальный индекс $\nu = 2$. Тогда множество прямых, содержащихся в S, является объединением двух таких множеств N_1, N_2, что всякая прямая из N_1 пересекается со всякой прямой из N_2, но никакие две различные прямые из N_1 (соответственно N_2) не пересекаются (упражнение 18г)). Пусть D, D' — две различные прямые из множества N_1; для всякого $z \in D$ существует единственная прямая $\Delta \in N_2$, проходящая через точку z; пусть $u(z)$ — точка, в которой прямая Δ пересекает D', показать, что u есть линейное проективное отображение прямой D на прямую D'.

д) Пусть $n = 3$ и D, D', D'' — три прямые проективного пространства $\boldsymbol{P}(E)$, из которых никакие две не пересекаются. Показать, что объединение прямых, пересекающих D, D' и D'', является невырожденной квадрикой.

24) В обозначениях и предположениях упражнения 23 предположим, что квадрика S не пуста и не вырождена.

а) Показать, что подгруппа Г проективной группы $\boldsymbol{PGL}(E)$, состоящая из проективных линейных биекций, переводящих S на себя, является каноническим образом группы подобий относительно формы Q. (Использовать упражнение 23в) § 6, упражнение 2а) § 4 и упражнение 8 § 1.)

б) Пусть точка $a \in \boldsymbol{P}(E)$ не принадлежит S и Φ_1 — сужение формы Ф на гиперплоскость, ортогональную в E к $\overline{\pi}^{-1}(a)$. Показать, что подгруппа группы Г, оставляющая точку a инвариантной, изоморфна факторгруппе ортогональной группы $U(\Phi_1)$ по ее центру.

в) Пусть b — точка S, F — (изотропная) гиперплоскость, ортогональная в E к $\overset{-1}{\pi}(b)$, M — (неизотропное) дополнение к $\overset{-1}{\pi}(b)$ относительно F, и Φ_2 — сужение формы Φ на M. Показать, что подгруппа группы Γ, оставляющая элемент b инвариантным, изоморфна группе подобий евклидова пространства L размерности $n-1$, имеющего форму, обратную к Φ_2, в качестве метрической формы (§ 1, n° 7). (Заметить, что если подобие относительно Φ переводит прямую $\overset{-1}{\pi}(b)$ на себя, то оно переводит гиперплоскость F на себя и полностью определяется своим сужением на F).

25) Пусть A — поле характеристики $\neq 2$, L — аффинное пространство над полем A конечной размерности $n \geqslant 2$. Пространство L отождествляется с дополнением к проективной гиперплоскости H_0 («бесконечно удаленной гиперплоскости») некоторого проективного пространства $\boldsymbol{P}(E)$ размерности n (гл. II, приложение III, n° 4). Непустое множество $S \subset L$ называется *аффинной квадрикой* (соответственно *аффинной коникой*, если $n=2$), если S является пересечением пространства L с некоторой проективной квадрикой (соответственно коникой) пространства $\boldsymbol{P}(E)$ (упражнение 23).

а) Пусть существует невырожденная проективная квадрика $\overline{S} \subset \boldsymbol{P}(E)$ такая, что $S = L \cap \overline{S}$. Показать, что такая квадрика единственна, исключение составляет лишь случай, когда $n=2$, $A = \boldsymbol{F}_3$ и S состоит из двух элементов (заметить, что при невыполнении условий указанного особого случая для всякой точки $z \in H_0$, не принадлежащей $\overline{S}$, существует прямая, проходящая через z и пересекающая S в двух различных точках). Тогда аффинную квадрику S называют невырожденной. Два аффинных линейных многообразия V_1, V_2, содержащихся в L, называются *сопряженными* относительно S, если проективные линейные многообразия $\overline{V}_1$, $\overline{V}_2$ такие, что $V_i = L \cap \overline{V}_i$ $(i=1, 2)$, сопряжены относительно $\overline{S}$; аналогично определяются *поляра* (в случае, когда она не содержится в H_0) и *полюс* аффинного линейного многообразия относительно S и аффинные линейные многообразия, *касательные* к S.

б) Пусть квадрика S невырождена; показать, что в пространстве L можно выбрать начало a таким образом, что после отождествления L с соответствующим векторным пространством в L найдется базис (e_i) такой, что множество S будет состоять из элементов $x = \sum_{i=1}^{n} \xi_i e_i$, удовлетворяющих уравнению одного из следующих двух видов:

$$\alpha_1 \xi_1^2 + \ldots + \alpha_n \xi_n^2 = 1,$$

$$\alpha_1 \xi_1^2 + \ldots + \alpha_{n-1} \xi_{n-1}^2 + \xi_n = 0.$$

В первом случае точка a однозначно определена и является полюсом бесконечно удаленной гиперплоскости H_0 относительно S. (Эта точка

называется *центром* квадрики S.) (Рассмотреть два случая: H_0 является или нет касательной к $\overline{S}$; применить и теорему 1 § 6, n° 1, и предложение 2 § 4, n° 2.)

26) Пусть A — алгебраически замкнутое поле характеристики $\neq 2$, E — конечномерное векторное пространство над полем A, Q — невырожденная квадратичная форма на пространстве E. Пусть $u \in \boldsymbol{O}(Q)$ в обозначениях упражнения 12 § 4, равенство $G(p, p) = \{0\}$ выполняется для всех $p \in A[X]$, кроме $p(X) = X - 1$ и $p(X) = X + 1$. Пусть M — минимальный элемент множества неизотропных подпространств, содержащихся в $G(p, p)$ и устойчивых относительно u, и p^h — минимальный многочлен сужения автоморфизма u на M; показать, что при нечетном h подмодуль M модуля E_u неразложим, а при четном h модуль M является прямой суммой двух изоморфных неразложимых подмодулей модуля E_u. (Чтобы убедиться, что при $h = 2k$ четном модуль M не может быть неразложимым, показать, что в этом случае подмодуль $N = p^k(u)(M)$ был бы вполне изотропным; взяв базис $(e_i)_{1 \leqslant i \leqslant 2k}$ модуля M, удовлетворяющий условию $u(e_i) = \varepsilon e_i + e_{i+1}$ при $i \leqslant 2k - 1$, $u(e_{2k}) = \varepsilon e_{2k}$ ($\varepsilon = \pm 1$), показать, что элемент e_k не может быть ортогонален к e_{k+1}, и вывести отсюда, что равенство $Q(u(e_k)) = Q(e_k)$ приводит к противоречию.)

27) Пусть A — поле характеристики 2, E — векторное пространство над полем A конечной размерности n, Q — квадратичная форма на пространстве E, Φ — билинейная форма, ассоциированная с формой Q. Форма Φ знакопеременная, так что ее ранг равен четному числу $2m$ (см. § 5, n° 1, следствие 1 теоремы 1).

а) Пусть E^0 — подпространство (размерности $n - 2m$) пространства E, ортогональное к E относительно Φ. Показать, что для любых векторов $x, y \in E^0$ выполняется равенство $Q(\lambda x + \mu y) = \lambda^2 Q(x) + \mu^2 Q(y)$; другими словами, сужение Q_0 формы Q на E_0 является отображением пространства E^0 (рассматриваемого как векторное пространство над полем A) в A (рассматриваемое как векторное пространство над подполем A^2), полулинейным относительно изоморфизма $\xi \to \xi^2$ поля A на A^2. Пусть q — размерность (над полем A) ядра $E^0 \cap \overset{-1}{Q}(0)$ формы Q, и E_1 — дополнение ядра $E^0 \cap \overset{-1}{Q}(0)$ относительно E^0; тогда справедливо неравенство $n - 2m - q \leqslant [A : A^2]$.

б) Вывести из а), что в пространстве E имеется базис $(e_i)_{1 \leqslant i \leqslant n}$, первые $2m$ векторов которого образуют базис дополнения E_2 подпространства E^0 в E, а следующие $n - 2m - q$ векторов образуют базис подпространства E_1; кроме того, при $x = \sum_{i=1}^{n} \xi_i e_i$

$$Q(x) = \sum_{i=1}^{m} (\alpha_i \xi_i^2 + \xi_i \xi_{m+i} + \beta_i \xi_{m+i}^2) + \sum_{i=2m+1}^{n-q} \gamma_i \xi_i^2,$$

где γ_i $(2m+1 \leqslant i \leqslant n-q)$ — элементы поля A, линейно независимые относительно подполя A^2.

в) Максимальная из размерностей вполне изотропных подпространств V пространства E, таких, что $V \cap E^0 = \{0\}$, называется *индексом* формы Q. Показать, что если индекс формы Q равен ν, то в пространстве E можно выбрать базис (e_i) таким образом, чтобы выполнялись свойства, указанные в б), откуда будет следовать, что $\alpha_i = \beta_i = 0$ при $1 \leqslant i \leqslant \nu$ и что сужение формы Q на подпространство, порожденное в e_2 векторами $e_{\nu+1}, \ldots, e_m, e_{m+\nu+1}, \ldots$ $\ldots, e_{2m}$, является (невырожденной) квадратичной формой индекса 0.

г) Предположим, что $q = 0$, и пусть $\boldsymbol{O}(Q)$ — группа автоморфизмов пространства E, оставляющих инвариантной форму Q, и $u \in \boldsymbol{O}(Q)$; показать, что $u(x) = x$ для любого $x \in E^0$. Для любого $x \in E_2$ положим $u(x) = u_0(x) + u_2(x)$, где $u_0(x) \in E^0$ и $u_2(x) \in E_2$; показать, что u_2 принадлежит симплектической группе $\mathbf{Sp}(\Phi_2)$ (где Φ_2 — сужение формы Φ на E_2); показать также, что $Q(u_2(x)) + Q(x) \in Q(E_0)$. Показать, что, обратно, для всякого автоморфизма $u_2 \in \mathbf{Sp}(\Phi_2)$, удовлетворяющего условию $Q(u_2(x)) + Q(x) \in Q(E_0)$ для всех $x \in E_2$, существует единственное линейное отображение u_0 подпространства E_2 в E^0 такое, что линейное отображение, равное $u_0 + u_2$ на E_2 и тождественное на E^0, принадлежит группе $\boldsymbol{O}(Q)$.

д) Предположим, что поле A *совершенно* $(A^2 = A)$ и $q = 0$. Вывести из б), что всякое векторное подпространство пространства E, размерность которого $\geqslant 3$, содержит по крайней мере один вектор x такой, что $Q(x) = 0$. Если n *нечетно*, то $m = \nu$, $n = 2m+1$, откуда следует, что в пространстве E имеется такой базис (e_i), что выполняется равенство

$$Q\Big(\sum_{i=1}^{n} \xi_i e_i\Big) = \xi_1\xi_{m+1} + \ldots + \xi_m\xi_{2m} + \xi_{2m+1}^2,$$

и (в обозначениях г)) группа $\boldsymbol{O}(Q)$ изоморфна $\mathbf{Sp}(\Phi_2)$; тогда все квадратичные формы такие, что $q = 0$, эквивалентны. Если n *четно*, то $n = 2m$, $\nu = m$ или $\nu = m-1$, и в пространстве E имеется такой базис (e_i), что выполняется равенство

$$Q\Big(\sum_{i=1}^{n} \xi_i e_i\Big) = \xi_1\xi_{m+1} + \ldots + \xi_{m-1}\xi_{2m-1} + \xi_m\xi_{2m} + \lambda(\xi_m^2 + \xi_{2m}^2), \qquad (1)$$

где $\lambda \in A$. Пусть A_1 — поле, полученное из A присоединением корней многочлена $\lambda X^2 + X + \lambda$; показать, что это поле не зависит от базиса, в котором форма Q может быть записана в виде (1); показать также, что для эквивалентности двух квадратичных форм (таких, что $q = 0$) необходимо и достаточно, чтобы соответствующие им таким способом квадратичные расширения поля A совпадали (применить теорему Витта). Разобрать случай, когда A — конечное поле характеристики 2.

*28) Пусть A — поле характеристики 2, отличное от F_2, E — векторное пространство размерности $n = 2m$ над полем A, Q — невырожденная квадратичная форма на E.

а) Показать, что ортогональная группа $\boldsymbol{O}(Q)$ порождается симметриями (которое представляют собой не что иное, как сдвиги, входящие в группу $\boldsymbol{O}(Q)$ (§ 4, упражнение 6)) (рассуждать, как в упражнении 11 § 5). Вывести отсюда, что коммутант группы $\boldsymbol{O}(Q)$ порождается квадратами элементов $\boldsymbol{O}(Q)$ (см. упражнение 17).

б) Предположим, что форма Q имеет максимальный индекс: пусть V, W — вполне сингулярные подпространства пространства E (§ 4, п° 1) размерности m, u — симметрия $x \to x + \dfrac{\Phi(x, a)}{Q(a)}\, a$ (§ 4, упражнение 6), k — размерность $V \cap W$. Показать, что размерность подпространства $V \cap u(W)$ равна $k + 1$, если вектор a ортогонален к $V \cap W$, и равна $k - 1$ в противоположном случае (в первом случае заметить, что $a = x + y$, где $x \in V$, $y \in W$, и показать, что $u(y) = x$; во втором случае заметить, что симметрия u не может оставить инвариантным ни один сингулярный вектор, не ортогональный к a).

в) Снова предположим, что индекс формы Q произволен. Показать, что подгруппа $\boldsymbol{SO}(Q)$ группы $\boldsymbol{O}(Q)$, состоящая из автоморфизмов пространства E, являющихся произведением *четного* числа симметрий, является в $\boldsymbol{O}(Q)$ нормальным делителем индекса 2. (Показать, что произведение нечетного числа симметрий не может быть равно единице, рассмотрев для этого продолжение формы Q на векторное пространство E', полученное из E расширением его поля скаляров до алгебраического замыкания; применить затем б).) (См. § 9, упражнение 9.)

г) Показать, что для любых двух вполне сингулярных подпространств V_1, V_2 пространства E, имеющих одинаковую размерность $< m$, существует автоморфизм $u \in \boldsymbol{SO}(Q)$ такой, что $u(V_1) = V_2$. Напротив, если V_1 и V_2 — вполне сингулярные подпространства размерности m, то автоморфизм $u \in \boldsymbol{SO}(Q)$ такой, что $u(V_1) = V_2$, существует тогда и только тогда, когда размерность подпространства $V_1 \cap V_2$ имеет ту же четность, что и m (рассуждать так же, как в упражнении 18; воспользоваться утверждением б)).

д) Плоскость $P \subset E$ называется *гиперболической*, если она неизотропна и содержит сингулярные прямые (обязательно две). Преобразование $u \in \boldsymbol{O}(Q)$ называется *гиперболическим*, если существует гиперболическая плоскость P такая, что $u(x) = x$ для всех $x \in P^0$; в этом случае u называется гиперболическим преобразованием, ассоциированным с плоскостью P. Показать, что если индекс формы Q строго положителен, то всякий автоморфизм $u \in \boldsymbol{O}(Q)$ является произведением гиперболических преобразований (использовать а)). Вывести отсюда, что если P — гиперболическая плоскость, то всякое преобразование $u \in \boldsymbol{O}(Q)$ может быть записано в виде $u = sv$, где $s \to$

гиперболическое преобразование, ассоциированное с P, и v принадлежит коммутанту группы $\boldsymbol{O}(Q)$.

29) В предположениях упражнения 28 будем считать дополнительно, что форма Q имеет максимальный индекс m; пусть (e_i) — симплектический базис пространства E (относительно знакопеременной формы Ф, ассоциированной с Q), состоящий из сингулярных векторов (§ 4, n° 2, предложение 2); отсюда следует, что матрица формы Ф относительно этого базиса совпадает с матрицей R из упражнения 14 § 5. Показать, что, в обозначениях этого упражнения, симплектическая матрица $({}^tD + S)^{-1}(D + S)$ тогда и только тогда является матрицей автоморфизма $u \in \boldsymbol{O}(Q)$, когда матрица S *знакопеременная* (заметив, что $({}^tD + S)\,u\,(e_i) = (D + S)\,e_i$, записать, что всякий вектор $u\,(e_i)$ сингулярен).

§ 7. Эрмитовы формы и упорядоченные поля

В § 7 K — некоторое *максимальное упорядоченное поле* (следовательно, это — поле характеристики 0; см. гл. VI, § 2) и рассматривается всегда один из трех следующих случаев:

1° $A = K$, J — тождественный автоморфизм,

2° A — поле $K(i)$, полученное из K присоединением квадратного корня i из -1, и для любого $\lambda \in A$ $\overline{\lambda}$ есть элемент, сопряженный к λ (гл. II, § 7, n° 7).

3° A — тело кватернионов над полем K, соответствующее паре $(-1, -1)$ (или, как мы будем для краткости говорить, *тело кватернионов над* K), и для всякого $\lambda \in A$ $\overline{\lambda}$ — элемент, сопряженный к λ (см. гл. II, § 7, n° 8 и гл. VIII, § 11, n° 2).

Если Ф — эрмитова форма на пространстве E, то в каждом случае $\Phi(x, x) \in K$ для всех $x \in E$, так как $\Phi(x, x) = \overline{\Phi(x, x)}$.

1. *Положительные эрмитовы формы*

Определение 1. *Эрмитова форма* Ф *на пространстве* E *называется положительной* (соответственно *отрицательной*), *если для любого* $x \in E$ *выполняется неравенство* $\Phi(x, x) \geqslant 0$ (соответственно $\Phi(x, x) \leqslant 0$).

В случае $A = K$ *положительной* (соответственно *отрицательной*) называют также квадратичную форму $Q(x) = \frac{1}{2}\Phi(x, x)$, с которой ассоциирована форма Ф.

Пусть пространство E конечномерно над телом A и (e_i) $(i = 1, \ldots, n)$ — ортогональный базис в E (§ 6, п° 1, теорема 1). Для того чтобы эрмитова форма Φ на пространстве E была положительной, необходимо и достаточно, чтобы $\Phi(e_i, e_i) \geqslant 0$ для любого $i = 1, \ldots, n$. Пусть Φ — *невырожденная положительная* форма на E. Поскольку всякий положительный элемент поля A является квадратом и, значит, имеет вид $\varrho\overline{\varrho}$ $(\varrho \in A)$, в E существуют ортонормальные базисы относительно Φ (§ 6, п° 1, следствие 1 теоремы 1).

Предложение 1. *Пусть E конечномерно и $A = K$ или $A = K(i)$. Если Φ — положительная невырожденная эрмитова форма на пространстве E, то ее продолжения на $\overset{p}{\otimes} E$ и $\overset{p}{\wedge} E$ $(p > 0)$, а также обратная форма являются положительными невырожденными эрмитовыми формами.*

Это утверждение сразу следует из существования в пространстве E ортонормального базиса и предложения 2 § 6, п° 1.

Предложение 1 остается верным, если повсюду в нем заменить слова «положительная невырожденная» на «положительная».

Предложение 2. *Пусть Φ — положительная эрмитова форма на E. Для любых $x, y \in E$ выполняется неравенство*

$$\Phi(x, y)\,\overline{\Phi(x, y)} \leqslant \Phi(x, x)\,\Phi(y, y). \qquad (1)$$

В самом деле, это неравенство очевидно, если векторы x и y пропорциональны. Предположим, что они независимы. Пусть A' — подполе $K(\Phi(x, y))$ тела A, F — векторная плоскость над A', порожденная элементами x и y, Φ_F — сужение формы Φ на F; эта форма Φ_F принимает значения в A'.

По предложению 1 дискриминант формы Φ_F относительно базиса (x, y) больше или равен нулю. Но этот дискриминант равен $\Phi(x, x)\,\Phi(y, y) - \Phi(x, y)\,\overline{\Phi(x, y)}$, что и требовалось доказать.

Следствие. *Множество изотропных векторов пространства E является подпространством E^0, ортогональным к E относительно Φ. Для того чтобы форма Φ была невырожденной, необходимо и достаточно, чтобы неравенство $\Phi(x, x) > 0$ выполнялось для всех $x \neq 0$.*

Предложение 3. *Пусть пространство E конечномерно, A коммутативно ($A = K$ или $A = K(i)$). Пусть, далее, Φ — эрмитова форма на E, X — матрица формы Φ относительно некоторого базиса (x_j) $(j = 1, \ldots, n)$ пространства E; для любого подмножества H отрезка $[1, n]$ обозначим через $X_{H,H}$ минор матрицы X, получаемый вычеркиванием строк и столбцов с номерами $j \in H$* (гл. III, § 6, n° 3).

а) *Если форма Φ невырождена и положительна, то для любого H $X_{H,H} > 0$.*

б) *Обратно, если $X_{H_j,H_j} > 0$ для любого $H_j = [1, j]$, то форма Φ невырождена и положительна.*

Предположим сначала, что форма Φ невырождена и положительна. Элементы (x_j) $(j \in H)$ образуют базис некоторого подпространства F в E, и минор $X_{H,H}$ является дискриминантом сужения Φ_F формы Φ на F относительно этого базиса; тогда, поскольку $\Phi_F(x, x) > 0$ для любого $x \neq 0$ в F, форма Φ_F невырождена и положительна (следствие предложения 2); поэтому $X_{H,H} > 0$ (предложение 1). Для доказательства б) заметим, что, в обозначениях предложения 1 § 6, n° 1, минор X_{H_j,H_j} равен $D_{j+1,j+1}$; следовательно, существует (предложение 1 § 6, n° 1) ортогональный базис (e_j) $(j = 1, \ldots, n)$ пространства E такой, что $\Phi(e_j, e_j) > 0$ для $j = 1, \ldots, n$; следовательно, форма Φ невырождена и положительна.

Замечание. Из существования ортонормальных базисов следует, что любые две невырожденные положительные эрмитовы формы над двумя векторными пространствами одинаковой размерности *эквивалентны* (§ 1, n° 6). Пусть тогда L — конечномерное эрмитово пространство над телом A, метрическая форма которого невырождена и положительна, и V_1 и V_2 — линейные многообразия в L *одинаковой* размерности (§ 6, n° 6); сужения метрической формы, с одной стороны, на направляющие подпространства T_1 и T_2 многообразий V_1 и V_2 и, с другой, на ортогональные подпространства T_1^0 и T_2^0 эквивалентны, так что существует унитарный автоморфизм u пространства переносов T пространства L такой, что $u(T_1) = T_2$ и $u(T_1^0) = T_2^0$; поэтому существует некоторое *движение v пространства L такое, что $v(V_1) = V_2$*. Пусть (a, b) и (a', b') — две пары точек из L; для того чтобы существовало

движение v пространства L такое, что $v(a) = a'$ и $v(b) = b'$, необходимо и достаточно, чтобы $e(a, b) = e(a', b')$ (обозначения те же, что и в § 6, n° 6); элемент $\sqrt{e(a, b)}$ кольца A (гл. VI, § 2, n° 2) называется *расстоянием* между точками a и b в эрмитовом пространстве L.

2. Закон инерции

Теорема 1 («закон инерции»). *Пусть A удовлетворяет условиям, сформулированным в начале § 7, пространство E конечномерно и Φ — эрмитова форма на E. Тогда:*

а) *существует разложение пространства E в прямую сумму подпространства E^0, ортогонального к E, и двух подпространств E^+ и E^- таких, что сужение формы Φ на E^+* (соответственно *на E^-*) *положительно* (соответственно *отрицательно*) *и не вырождено;*

б) *пространство E имеет ортогональный базис $(e_i)_{1 \leqslant i \leqslant n}$ такой, что*

$$\Phi\Big(\sum_{i=1}^{n} \xi_i e_i,\ \sum_{i=1}^{n} \eta_i e_i\Big) = \sum_{i=1}^{s} \xi_i \bar{\eta}_i - \sum_{i=s+1}^{s+t} \xi_i \bar{\eta}_i; \tag{2}$$

в) *для любых разложений пространства E в прямую сумму подпространств, удовлетворяющих условиям* а), *размерности s подпространств E^+ (и t подпространств E^-) одинаковы; целое число s* (соответственно t) *является максимумом размерностей подпространств F пространства E таких, что сужение формы Φ на F невырождено и положительно* (соответственно *отрицательно*);

г) *ранг формы Φ равен $s + t$;*

д) *если форма Φ невырождена, то ее индекс равен* $\inf(s, t)$ (§ 4, n° 2, определение 3).

В самом деле, пусть (x_i) $(i = 1, \ldots, n)$ — ортогональный базис пространства E (§ 6, n° 1, теорема 1); вспомним, что $\Phi(x, x) \in K$ для любого $x \in E$. Можно считать, что $\Phi(x_i, x_i) > 0$ для $i = 1, \ldots, s$, $\Phi(x_i, x_i) < 0$ для $i = s + 1, \ldots, s + t$ и $\Phi(x_i, x_i) = 0$ для $i = s + t + 1, \ldots, n$.

Обозначив через E^+ (соответственно E^-) подпространство, порожденное векторами $x_1, \ldots, x_s$ (соответственно $x_{s+1}, \ldots, x_{s+t}$), мы получим утверждение а), так как векторы

$x_{s+t+1}, \ldots, x_n$ порождают подпространство E^0. Так как для $i = 1, \ldots, s$ (соответственно $i = s+1, \ldots, s+t$) элемент $\Phi(x_i, x_i)$ имеет вид $\varrho\bar{\varrho}$ (соответственно $-\varrho\bar{\varrho}$) ($\varrho \in A^*$), то отсюда следует утверждение б). Для доказательства в) рассмотрим такое подпространство P в E, что сужение формы Φ на P невырождено; тогда $P \cap (E^- + E^+) = \{0\}$ и, следовательно, сумма $P + E^- + E^+$ прямая; отсюда следует, что $\dim P \leqslant \dim E^+ = s$, что доказывает утверждение в). Утверждение г) немедленно следует из а).

Предположим, наконец, что форма Φ невырождена, положим $q = \inf(s, t)$ и покажем, что q — индекс формы Φ. В обозначениях б), векторы $e_i + e_{s+i}$ (соответственно $e_i - e_{s+i}$) ($i = 1, \ldots, q$) порождают вполне изотропное подпространство F (соответственно F'). Так как характеристика поля K равна нулю, то сумма $F + F'$ порождается векторами $e_1, \ldots, e_q, e_{s+1}, \ldots, e_{s+q}$ и, следовательно, неизотропна. Тогда сужение формы Φ на подпространство $H = (F + F')^0$ невырождено и положительно (соответственно отрицательно), так что H не содержит ненулевых неизотропных векторов. Поскольку подпространство F^0 содержит подпространства F и H и $\dim(F + H) = \operatorname{codim} F' = \operatorname{codim} F$, то $F^0 = F + H$. Стало быть, всякий изотропный вектор z, ортогональный к подпространству F, должен лежать в F, так как компонента в H вектора z из прямой суммы $F + H$ изотропна. Следовательно, F — максимальное вполне изотропное подпространство, что и доказывает д).

Определение 2. *Пара* (s, t) *(в обозначениях теоремы* 1*) называется сигнатурой формы* Φ.

3. *Приведение формы по отношению к данной положительной эрмитовой форме*

В этом п° предполагается, что пространство E имеет конечную размерность n над телом A, а эрмитова форма Φ на пространстве E *невырождена и положительна.*

Так как линейные отображения пространства E в E^*, ассоциированные с формой Φ, биективны, то для любых элементов $x, y, z \in E$, $y \neq 0$, существует единственный элемент $t \in E$ такой,

что $\Phi(x, z) = \overline{\Phi(t, y)}$. В частности, *если* $A = K$ или $A = K(i)$ и u — *полулинейное* относительно J отображение пространства E в себя (гл. II, приложение I, n° 1), то для любого $x \in E$ существует единственный элемент $u^*(x)$ такой, что для всех $y \in E$ выполняется равенство $\Phi(x, u(y)) = \overline{\Phi(u^*(x), y)}$. Ясно, что u^* является полулинейным относительно J отображением пространства E в себя; это отображение называется *сопряженным* к отображению u.

Замечания. 1) Если J — тождественный автоморфизм, мы приходим к понятию сопряженного гомоморфизма, введенному в § 1, n° 8.

2) Пусть $A = K$ или $A = K(i)$, E^J — правый A-модуль, определенный в § 1, n° 2, определение 5. Φ является билинейной формой на произведении $E \times E^J$, Φ^J — билинейной формой на произведении $E^J \times E$, u — A-линейным отображением модуля E в E^*. Сопряженный к u гомоморфизм в смысле § 1, n° 8, будет тогда A-линейным отображением модуля E в E^*. Очевидно, это отображение совпадает с отображением u^*, определенным выше.

Эндоморфизм u пространства E называется *нормальным* (относительно Φ), если $uu^* = u^*u$.

Примеры нормальных эндоморфизмов.

1) *Унитарные* автоморфизмы (§ 6, n° 2), характеризующиеся равенством $u^{-1} = u^*$ (§ 1, n° 8, следствие предложения 8);

2) эндоморфизмы u, удовлетворяющие условию $u = u^*$; эти эндоморфизмы называются *эрмитовыми*.

Для всякого эндоморфизма u пространства E положим $\Phi_u(x, y) = \Phi(u(x), y)$; тогда

$$\Phi_u(y, x) = \Phi(u(y), x) = \Phi(y, u^*(x)) = \overline{\Phi(u(x), y)} = \overline{\Phi_u(x, y)},$$

то есть форма Φ_u на пространстве E эрмитова. Обратно, пусть Ψ — эрмитова форма на пространстве E; так как отображение s_Φ пространства E в E^*, ассоциированное с формой Φ, биективно, то для любого $x \in E$ существует единственный элемент $u(x) \in E$ такой, что $\Psi(x, y) = \Phi(u(x), y)$. Легко проверить, что u является эрмитовым эндоморфизмом пространства. Таким образом, отображение $u \to \Phi_u$ является биекцией множества эрмитовых эндоморфизмов пространства E на множество эрмитовых форм на E и называется *канонической биекцией*.

Пусть $A = K$ или $A = K(i)$; если на пространстве E задана *билинейная* форма Ψ, то для любого $x \in E$ существует единственный элемент $u(x) \in E$ такой, что $\Psi(x, y) = \overline{\Phi(u(x), y)}$; ясно, что u будет *полулинейным* (относительно J) отображением пространства E в себя. Так как $\overline{\Phi(u(x), y)} = \Phi(y, u(x)) = \overline{\Phi(u^*(y), x)}$, то форма Ψ является симметрической (соответственно знакопеременной) тогда и только тогда, когда $u^* = u$ (соответственно $u^* = -u$).

Теорема 2. *Пусть S — множество эндоморфизмов пространства E* (соответственно *полулинейных отображений E в себя, если $A = K$ или $A = K(i)$*), *устойчивое относительно отображения $u \to u^*$. Если подпространство $V \subset E$ устойчиво относительно множества S, то его ортогональное дополнение устойчиво относительно S. Далее, пространство E является прямой суммой попарно ортогональных подпространств, устойчивых относительно S и минимальных во множестве ненулевых устойчивых относительно S подпространств.*

В самом деле, пусть подпространство V в E устойчиво относительно S; для любых $x \in V^0$, $y \in V$ и $u \in S$ имеем $u^*(y) \in V$, откуда $\Phi(y, u(x)) = \Phi(u^*(y), y) = 0$ (соответственно $\Phi(y, u(x)) = \overline{\Phi(u^*(y), x)} = 0$), и следовательно, $u(x) \in V^0$; таким образом, подпространство V^0 устойчиво относительно множества S, что доказывает первое утверждение. Для доказательства второго утверждения проведем индукцию по размерности n пространства E. Случай $n = 0$ тривиален. Если $n \neq 0$, то в E существует минимальное подпространство $V \neq \{0\}$, устойчивое относительно S, например ненулевое устойчивое подпространство минимальной размерности. Теперь достаточно применить предположение индукции к V^0, поскольку сопряженный эндоморфизм к сужению эндоморфизма u на V^0 (относительно сужения формы Φ) совпадает с сужением на V^0 эндоморфизма, сопряженного к u.

Следствие 1. *Пусть $A = K$ или $A = K(i)$, и B — подалгебра в $\mathfrak{L}_A(E)$, устойчивая относительно отображения $u \to u^*$. Тогда пространство E является полупростым B-модулем и разлагается в прямую сумму попарно ортогональных простых подмодулей. Алгебра B полупроста.*

В самом деле, поскольку каждый B-подмодуль V пространства E имеет дополнение, например V^0, B-модуль E полупрост (гл. VIII, § 3, n° 3, предложение 7). Так как всякий минимальный ненулевой B-подмодуль пространства E простой, E является прямой суммой попарно ортогональных простых подмодулей. Наконец, алгебра B полупроста, так как она имеет точный полупростой модуль E, контрмодуль которого является модулем конечного типа (гл. VIII, § 5, n° 1, предложение 3).

Следствие 2. *В обозначениях и предположениях следствия 1 будем считать дополнительно, что алгебра B коммутативна. Тогда все ее элементы являются полупростыми (нормальными) эндоморфизмами пространства E. В случае $A = K$* (соответственно $A = K(i)$) *E является прямой суммой попарно ортогональных простых B-подмодулей, являющихся векторными пространствами размерности* 1 *или* 2 (соответственно 1) *над полем A.*

Первое утверждение следует из предложения 2 гл. VIII, § 9, n° 1, так как алгебра B полупроста. С другой стороны, всякий простой B-модуль изоморфен B-модулю вида $B/\mathfrak{m}$, где $\mathfrak{m}$ — максимальный идеал алгебры B, то есть изоморфен полю L конечной степени над полем A; в случае $A = K$ (соответственно $A = K(i)$) поле L изоморфно K или $K(i)$ (соответственно $K(i)$), так как поле $K(i)$ алгебраически замкнуто (гл. VI, § 2, n° 3, теорема 3).

Предложение 4. *Пусть u — нормальный эндоморфизм пространства E. В случае, когда A есть $K(i)$ или тело кватернионов над полем K, E имеет ортонормальный (относительно Ф) базис, состоящий из собственных векторов эндоморфизма u. В случае $A = K$ эндоморфизм полупрост и E является прямой суммой попарно ортогональных подпространств размерности* 1 *или* 2, *устойчивых относительно u.*

Рассмотрим сначала случай, когда A коммутативно ($A = K$ или $A = K(i)$). Тогда подалгебра $B = A[u, u^*]$ в $\mathscr{L}_A(E)$ коммутативна, так как эндоморфизм u нормален; по формулам (32) и (33) § 1, n° 8, подалгебра B устойчива при отображении $v \to v^*$. В случае $A = K$ утверждение немедленно следует тогда из следствия 2 теоремы 2. В случае $A = K(i)$ это следствие показывает, что E является прямой суммой попарно ортогональных векторных

подпространств Ax_i $(i = 1, \ldots, n)$ размерности 1, устойчивых относительно эндоморфизма u; положив $e_i = \Phi(x_i, x_i)^{-\frac{1}{2}} x_i$, получим искомый ортонормальный базис (e_i).

В случае, когда A — тело кватернионов над полем K, достаточно показать, ввиду теоремы 2, что всякий минимальный элемент множества ненулевых подпространств, устойчивых относительно эндоморфизмов u и u^*, имеет размерность 1. Но всякое такое подпространство V содержит собственный вектор $x \neq 0$ эндоморфизма u *): в этом легко убедиться, если заметить, что тело кватернионов A содержит алгебраически замкнутое подполе $K(i)$, и сузить тело скаляров пространства V до этого подполя. Теперь остается лишь показать, что собственный вектор x эндоморфизма u является собственным и для эндоморфизма u^*. Пусть $u(x) = ax$ $(a \in A)$; тогда $\Phi(u(x), x) = a\Phi(x, x) = \Phi(x, x)\, a = \Phi(x, \bar{a}x)$, так как элемент $\Phi(x, x)$ входит в центр тела A; с другой стороны, $\Phi(u(x), x) = \Phi(x, u^*(x))$; отсюда следует, что $\Phi(x, u^*(x) - \bar{a}x) = 0$, так что можно записать $u^*(x) = \bar{a}x + z$, где z — вектор, ортогональный к x. Но тогда

$$\Phi(u^*(x), u^*(x)) = \bar{a}a\Phi(x, x) + \Phi(z, z) = \Phi(u(x), u(x)) + \Phi(z, z).$$

Поскольку эндоморфизм u нормален, то

$$\Phi(u(x), u(x)) = \Phi(x, u^*u(x)) = \Phi(x, uu^*(x)) = \Phi(uu^*(x), x) = \Phi(u^*(x), u^*(x)).$$

Следовательно, $\Phi(z, z) = 0$, откуда, по предположению, $z = 0$ и $u^*(x) = \bar{a}x$, что и требовалось доказать.

Замечание. Из теоремы 2 следует, что собственные подпространства, соответствующие двум различным собственным значениям эндоморфизма u, ортогональны.

Предложение 5. *Пусть u — эрмитов эндоморфизм пространства E. Собственные значения эндоморфизма u принадлежат полю K.*

*) Пусть E — левое векторное пространство над некоммутативным телом A и u — эндоморфизм пространства E; вектор $x \neq 0$ из E называется *собственным вектором* эндоморфизма u, если существует элемент $a \in A$ такой, что $u(x) = ax$; скаляр a называется тогда *собственным значением* эндоморфизма u. Заметим, что для любого $b \neq 0$ из кольца A вектор bx будет собственным вектором эндоморфизма u и соответствующее собственное значение равно bab^{-1}.

и пространство E имеет ортонормальный базис, составленный из собственных векторов эндоморфизма u.

В случае, когда A есть поле $K(i)$ или тело кватернионов над полем K, достаточно, ввиду предложения 4, доказать первое утверждение; однако если x — ненулевой собственный вектор эндоморфизма u и a — соответствующее собственное значение, то по условию $u = u^*$ имеем

$$a\Phi(x, x) = \Phi(u(x), x) = \Phi(x, u(x)) = \Phi(x, x)\,\bar{a}.$$

Так как $\Phi(x, x)$ — ненулевой элемент центра кольца A, то из этого равенства следует, что $a = \bar{a}$, то есть $a \in K$. Следовательно, все собственные значения эрмитовой матрицы лежат в поле K. Теперь рассмотрим случай $A = K$. Матрица M эндоморфизма u относительно любого ортонормального базиса пространства E будет тогда симметрической, то есть эрмитовой, если ее рассматривать как матрицу над $K(i)$. Первая часть доказательства показывает, что все собственные значения этой матрицы лежат в K, так что если $E \neq \{0\}$, то матрица M имеет в E ненулевые собственные векторы. Отсюда следует, что всякое минимальное подпространство, устойчивое относительно эндоморфизма u, имеет размерность 1, откуда, как в предложении 4, легко следует доказываемое утверждение.

Предложение 6. а) *Пусть Ψ — эрмитова форма* (соответственно *симметрическая билинейная форма, если $A = K$ или $A = K(i)$*) *на пространстве E. Тогда в E существует базис, ортонормальный относительно Φ и ортогональный относительно Ψ.*

б) *Пусть $A = K$ или $A = K(i)$, и Ψ — знакопеременная билинейная форма на пространстве E. Тогда в E существует ортонормальный* (*относительно Φ*) *базис, относительно которого матрица формы Ψ имеет вид*

$$\begin{pmatrix} 0 & a_1 & 0 & 0 & \dots & 0 \\ -a_1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & a_2 & \dots & 0 \\ 0 & 0 & -a_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix},$$

где все $a_i \geqslant 0$ в поле K.

Для эрмитовой формы Ψ наше утверждение легко следует из предложения 5 и канонического соответствия между эрмитовыми формами на пространстве E и эрмитовыми эндоморфизмами относительно формы Φ. В двух оставшихся случаях возьмем полулинейное отображение u пространства E в себя, определенное в начале этого n° формулой $\Psi(x, y) = \overline{\Phi(u(x), y)}$. Тогда отображение u^2 A-линейно; если форма Ψ симметрическая (соответственно знакопеременная), то $u = u^*$ (соответственно $u = -u^*$), так что эндоморфизм u^2 эрмитов, отсюда следует

$$\Phi(u^2(x), x) = \overline{\Phi(x, u^2(x))} = \Phi(u^*(x), u(x)) = \Phi(u(x), u(x))$$

(соответственно $-\Phi(u(x), u(x))$),

то есть эрмитова форма $(x, y) \to \Phi(u^2(x), y)$ положительна (соответственно отрицательна). Применим теперь теорему 2 и обозначим через V минимальный элемент множества ненулевых подпространств в E, устойчивых относительно эндоморфизмов u и u^*. Поскольку эндоморфизм u^2 эрмитов, подпространство V содержит некоторый его собственный вектор $x \neq 0$; положим $u^2(x) = ax$, где $a \in K$ (предложение 5).

Если Ψ — форма симметрическая, то неравенство $\Phi(u^2(x), x) \geqslant 0$ показывает, что $a \geqslant 0$. Положим $y = a^{1/2}x + u(x)$; тогда $u(y) = a^{1/2}u(x) + ax = a^{1/2}y$ и, значит, подпространство Ay устойчиво относительно эндоморфизмов u и u^*. Если $y = 0$, то устойчивым относительно u и u^* будет подпространство Ax; во всяком случае, подпространство V имеет размерность 1, так что наше утверждение сразу следует из теоремы 2.

Если Ψ — знакопеременная форма, то $a \leqslant 0$; положим

$$y = (-a)^{1/2}x + u(x), \qquad z = (-a)^{1/2}x - u(x).$$

Тогда $u(y) = -(-a)^{1/2}z$, $u(z) = (-a)^{1/2}y$ и

$$\Phi(y, z) = -a\Phi(x, x) - \Phi(u(x), u(x)) = -\Phi(ax, x) + \Phi(u^2(x), x) = 0.$$

Если $y = z = 0$, то $a = 0$ и $u(x) = 0$, так что подпространство Ax устойчиво относительно u и u^*, V имеет размерность 1, и матрица сужения формы Ψ на V нулевая, так как форма Ψ знакопеременная. Если же оба элемента y и z отличны от 0, то они порождают пространство V, которое, в силу ортогональности

векторов y и z, имеет размерность 2. Матрица сужения формы Ψ на V имеет при этом вид $\begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}$. Наконец, в силу формулы $\Psi(x', y') = \overline{\Phi(u(x'), y')}$ имеем равенство $\Psi(x', y') = 0$, если x' и y' принадлежат двум подпространствам, устойчивым относительно эндоморфизма u и ортогональным относительно Φ. Отсюда следует существование ортонормального (относительно Φ) базиса пространства E, относительно которого матрица формы Ψ имеет указанный вид, что и требовалось доказать.

Упражнения. 1) Пусть выполнены предположения, указанные в начале § 7, и Φ — положительная эрмитова форма на пространство E.

а) Для выполнения равенства $\Phi(x, x)\,\Phi(y, y) = \Phi(x, y)\,\overline{\Phi(x, y)}$ необходимо и достаточно, чтобы векторы x и y были зависимы или порожденная ими плоскость была изотропна.

б) Предположим, что для всякого $x \in E$ элемент $\Phi(x, x)$ является в поле K квадратом. Показать, что для любых двух векторов $x, y \in E$ справедливо неравенство

$$\sqrt{\Phi(x+y, x+y)} \leqslant \sqrt{\Phi(x, x)} + \sqrt{\Phi(y, y)}.$$

Если форма Φ невырождена, то левая и правая части этого неравенства могут быть равны только в случае, когда $\alpha x + \beta y = 0$, где α и β — элементы поля K, не равные одновременно нулю, и $\alpha\beta \leqslant 0$.

2) Предположим, что $A = K$ или $A = (K(i)$, и пусть X — эрмитова квадратная матрица порядка n над A такая, что $X_{H,H} \geqslant 0$ для любого непустого подмножества H отрезка $[1, n]$. Обозначения из предложения 3 § 1.

а) Пусть $\lambda > 0$ — элемент поля K; показать, что матрица $X + \lambda I$ положительная невырожденная (применить предложение 3 n° 1 и индукцию по n).

б) Вывести отсюда, что эрмитова матрица X *положительна.*

3) Предположим, что $A = K$ или $A = K(i)$ и пространство конечномерно. Пусть Φ_1, Φ_2 — положительные эрмитовы формы на E, $V = (\alpha_{ij})$, $W = (\beta_{ij})$ — матрицы этих форм относительно одного и того же базиса (e_i) пространства E. Пусть, далее, форма Φ имеет относительно базиса (e_i) матрицу (γ_{ij}), где $\gamma_{ij} = \alpha_{ij}\beta_{ij}$ для любых индексов i и j. Показать, что форма Φ положительна и, кроме того, если Φ_1 и Φ_2 невырождены, то и Φ невырождена. (При вычислении $\Phi(x, x)$ выразить элементы α_{ij} через $\Phi_1(c_i, c_i)$, где (c_i) — базис пространства E, ортогональный относительно формы Φ_1.)

4) Предположим, что $A = K$ или $A = K(i)$. Пусть R — эрмитова матрица порядка n над полем A, и пусть эрмитова форма на про-

странстве A^n, имеющая в каноническом базисе матрицу R, имеет сигнатуру (s, t); тогда (s, t) называют сигнатурой матрицы R. Обозначим через Δ_k главный минор матрицы R, полученный вычеркиванием из R строк и столбцов с номерами $> k$; предположим, что $\Delta_{s+t} \neq 0$ и для всякого $k < s + t$ миноры Δ_k и Δ_{k+1} не равны нулю одновременно (см. § 6, упражнение 1б)). Показать, что если для некоторого $k < s + t$ минор $\Delta_k = 0$, то Δ_{k-1} и Δ_{k+1} имеют противоположные знаки (так же, как в упражнении 1а) § 6) и выполняется равенство

$$s - t = \operatorname{sgn} \Delta_1 + \operatorname{sgn} (\Delta_1\Delta_2) + \ldots + \operatorname{sgn} (\Delta_{s+t-1}\Delta_{s+t})$$

(воспользоваться упражнением 2 § 6).

5) Предположим, что $A = K$ или $A = K(i)$; пусть R, S — эрмитовы матрицы над полем A с сигнатурами (s, t) и (s', t') соответственно (упражнение 4); показать, что матрица $R \otimes S$ эрмитова и ее сигнатура равна $(ss' + tt', st' + s't)$.

6) Пусть K — максимальное упорядоченное поле, L — простая алгебра конечного ранга над полем K, (s, t) — сигнатура симметрической билинейной формы $(x, y) \to \operatorname{Tr}_{L/K}(xy)$ на алгебре L. Показать, что

$s - t = m$, если алгебра L изоморфна алгебре матриц порядка m над полем K;

$s - t = 0$, если L изоморфна алгебре матриц над $K(i)$;

$s - t = -2m$, если L изоморфна алгебре матриц порядка m над телом кватернионов над полем K.

7) Предположим, что A удовлетворяет условиям, указанным в начале § 7, и пространство E имеет конечную размерность n.

Пусть Φ — невырожденная положительная эрмитова форма на E.

а) Показать, что всякое подобие относительно Φ единственным образом может быть представлено в виде произведения гомотетии с коэффициентом $\geqslant 0$ в поле K и унитарного преобразования.

б) Показать, что для всякого базиса $(a_i)_{1 \leqslant i \leqslant n}$ пространства E найдется единственный ортонормальный базис $(e_i)_{1 \leqslant i \leqslant n}$ этого пространства, удовлетворяющий следующим условиям: 1° для любого m, $1 \leqslant m \leqslant n$, подпространство, порожденное векторами $a_1, \ldots, a_m$, совпадает с подпространством, порожденным векторами $e_1, \ldots, e_m$; 2° для всех индексов i выполняется неравенство $\Phi(a_i, e_i) > 0$ в поле K (см. § 6, n° 1, предложение 1).

в) Пусть M — обратимая квадратичная матрица порядка n над полем A; вывести из б), что существует единственная пара (L, U) матриц порядка n таких, что U унитарна, и все элементы матрицы $L = (\lambda_{ij})$, лежащие ниже главной диагонали, равны нулю, а ее диагональные элементы $\lambda_{ii} > 0$ в поле K и, наконец, $M = LU$.

* 8) Предположим, что $A = K$; пусть L — конечномерное эрмитово пространство над полем A и его метрическая форма положительна и невырождена. Пусть u — биекция некоторого подмножества M на

подмножество N такая, что для любых точек a, $b \in M$ выполняется равенство $e(u(a), u(b)) = e(a, b)$. Показать, что найдется движение, сужение которого на M равно u (так же, как в процессе ортогонализации Грама — Шмидта, провести индукцию по размерности аффинного линейного многообразия, порожденного множеством M). Можно ли перенести это предложение на случай, когда A есть $K(i)$ или тело кватернионов над полем K?

9) Пусть выполнены условия, указанные в § 3; предположим дополнительно, что A есть тело кватернионов над полем K. Пусть u — нормальный эндоморфизм пространства E. Показать, что пространство E является прямой суммой попарно ортогональных подпространств F_k $(1 \leqslant k \leqslant r)$, в каждом из которых существует ортонормальный базис (e_{ik}) $(1 \leqslant i \leqslant n_k)$, причем $u(e_{ik}) = \lambda_k e_{ik}$ при $1 \leqslant i \leqslant n_k$ и два элемента λ_k с различными индексами не могут быть переведены друг в друга никаким внутренним автоморфизмом тела A. Более того, если (F'_k) — другое разложение пространства E, обладающее теми же свойствами, с системой (λ'_k) собственных значений, то (с точностью до перестановки индексов) $F'_k = F_k$ и $\lambda'_k = \alpha_k \lambda_k \alpha_k^{-1}$; множество собственных векторов эндоморфизма u, соответствующих собственному значению λ_k, является подпространством над централизатором A_k элемента λ_k в теле A и порождается векторами e_{ik} $(1 \leqslant i \leqslant n_k)$.

10) Пусть выполнены условия, указанные в § 3; предположим дополнительно, что A есть $K(i)$ или тело кватернионов над полем K. Пусть u — нормальный эндоморфизм пространства E.

а) Показать, что векторное подпространство F пространства E обладает свойством $u(F) \subset F$ тогда и только тогда, когда оно порождается собственными векторами эндоморфизма u; в этом случае $u(F^0) \subset F^0$ и $u^*(F) \subset F$.

б) Эндоморфизм u унитарный (соответственно $u^* = u$, $u^* = -u$) тогда и только тогда, когда все его собственные значения λ удовлетворяют уравнению $\lambda\bar{\lambda} = 1$ (соответственно $\bar{\lambda} = \lambda$, $\bar{\lambda} = -\lambda$).

в) Эрмитов эндоморфизм u пространства E называется *положительным* (соответственно *невырожденным положительным*), если канонически соответствующая ему эрмитова форма $(x, y) \to \Phi(u(x), y)$ положительна (соответственно невырождена и положительна); для этого необходимо и достаточно, чтобы все собственные значения эндоморфизма u были $\geqslant 0$ (соответственно > 0).

г) Показать, что для любого целого числа m существует нормальный эндоморфизм v пространства E такой, что $v^m = u$. Если u — положительный эрмитов эндоморфизм, то существует единственный положительный эрмитов эндоморфизм v такой, что $v^m = u$, и существует многочлен $f \in K[X]$ такой, что $v = f(u)$; последнее утверждение верно и в случае $A = K$.

11) Пусть выполнены условия, указанные в n° 3; предположим дополнительно, что $A = K$. Пусть u — нормальный эндоморфизм пространства E.

а) Пусть V — минимальный элемент множества ненулевых подпространств пространства E, устойчивых относительно u и u^*; показать, что если размерность подпространства V равна 2, то сужение эндоморфизма u на V является прямым подобием с коэффициентом > 0.

б) Показать, что всякое подпространство, устойчивое относительно u, устойчиво также и относительно u^*. (Пусть E_0 — векторное пространство, полученное из E расширением поля скаляров до $K(i)$; форма Ф является сужением на E некоторой невырожденной положительной эрмитовой формы на пространстве E_0, эндоморфизм u является сужением нормального эндоморфизма (относительно этой формы) u_0 пространства E_0; кроме того, E является множеством элементов $x \in E_0$, инвариантных относительно инволютивной полулинейной биекции j пространства E_0, и $u_0 j = j u_0$. Затем применить упражнение 10а).)

12) Пусть выполнены условия, указанные в n° 3; предположим дополнительно, что A есть $K(i)$ или тело кватернионов над полем K. Показать, что для всякого эндоморфизма u пространства E найдется ортонормальный базис этого пространства, относительно которого u имеет матрицу со всеми нулями ниже диагонали. (Рассмотрев некоторый собственный вектор эндоморфизма u, применить индукцию по размерности пространства E.)

13) Пусть A — тело, удовлетворяющее условиям, указанным в начале § 7, E, F — конечномерные векторные пространства над A, Ф (соответственно Ψ) — невырожденная положительная эрмитова форма на пространстве E (соответственно F), u — линейное отображение пространства E в F. Показать, что отображения u^*u и uu^*, где u^* — сопряженное к u отображение (относительно Ф и Ψ; см. § 1, n° 8), являются положительными (см. упражнение 10в)) эрмитовыми эндоморфизмами пространств E и F соответственно.

14) Пусть выполнены условия, указанные в § 7 n° 3. Пусть u — эндоморфизм пространства E, h_1, h_2 — положительные эрмитовы эндоморфизмы пространства E, причем $h_1^2 = u^*u$, $h_2^2 = uu^*$ (упражнения 13 и 10г)).

а) Показать, что существует унитарный эндоморфизм v такой, что $u = vh_1 = h_2 v$, и, в частности, эндоморфизмы h_1 и h_2 подобны (заметить, что $\overset{-1}{u}(0) = \overset{-1}{h_1}(0)$ и что равенство $\Phi(u(x), u(x)) = \Phi(h_1(x), h_1(x))$ выполняется для всех векторов x подпространства V, ортогонального к $\overset{-1}{u}(0)$). Эндоморфизм v определяется однозначно тогда и только тогда, когда u биективен. Для того чтобы можно было найти эндоморфизм v, перестановочный с h_1, необходимо и достаточно, чтобы u был нормальным.

б) Вывести из а), что всякая квадратная матрица M порядка n над полем A может быть представлена в виде UDV, где U и V — унитарные матрицы, D — диагональная матрица, у которой все диагональные элементы $\geqslant 0$, причем их квадраты являются собственными значениями матрицы MM^*.

15) Пусть выполнены условия, указанные в n° 3. Показать, что всякая положительная матрица H эрмитова над полем A и может быть представлена в виде LL^*, где в матрице L все элементы ниже диагонали равны нулю, а диагональные элементы принадлежат K и > 0; кроме того, если матрица H обратима, то L определяется однозначно (см. упражнения 10г) и 7в)).

*16) Пусть выполнены условия, указанные в n° 3, и $A = K(i)$. Пусть u — эндоморфизм пространства E.

а) Множество собственных значений эндоморфизма u содержится в множестве U значений формы $\Phi(x, u(x))$, когда x пробегает множество элементов пространства E таких, что $\Phi(x, x) = 1$.

б) Подмножество C поля $A = K(i)$ называется *выпуклым*, если для любой пары элементов $(\xi, \eta) \in C^2$ и любого $\tau \in K$ такого, что $0 \leqslant \tau \leqslant 1$, элемент $\tau\xi + (1 - \tau)\eta \in C$. Показать, что множество U выпукло. (Свести доказательство к случаю $n = 2$; записав u в виде $v + iw$, где v и w — эрмитовы эндоморфизмы, и заменяя при необходимости u на λu, где $\lambda \in A$ и $\lambda\bar{\lambda} = 1$, показать, что задача сводится к доказательству следующего свойства. Пусть $f(\xi_1, \xi_2) = \xi_1\bar{\xi}_1 + \xi_2\bar{\xi}_2$, $g(\xi_1, \xi_2) = a\xi_1\bar{\xi}_1 + b\xi_2\bar{\xi}_2$ $(a \in K, b \in K)$; $h(\xi_1, \xi_2) = \alpha\xi_1\bar{\xi}_1 + \beta\xi_1\bar{\xi}_2 + \bar{\beta}\xi_2\bar{\xi}_1 + \gamma\xi_2\bar{\xi}_2$ $(\alpha \in K, \gamma \in K, \beta \in A)$; пусть $(\eta_1, \eta_2) \in A^2$, $(\zeta_1, \zeta_2) \in A^2$ и $f(\eta_1, \eta_2) = f(\zeta_1, \zeta_2) = 1$, $g(\eta_1, \eta_2) = g(\zeta_1, \zeta_2) = 1$, $h(\eta_1, \eta_2) > 0$, $h(\zeta_1, \zeta_2) < 0$; тогда существует пара $(\vartheta_1, \vartheta_2) \in A^2$ такая, что $f(\vartheta_1, \vartheta_2) = 1$, $g(\vartheta_1, \vartheta_2) = 1$, $h(\vartheta_1, \vartheta_2) = 0$. Сначала заметить, что для любой пары (ξ_1, ξ_2) существует элемент $\mu \in A$ такой, что $\mu\bar{\mu} = 1$ и $\beta\mu\xi_1\bar{\xi}_2 + \bar{\beta}\mu\xi_2\bar{\xi}_1 = 0$; это позволит свести доказательство к случаю $\beta = 0$; применить предложение 5, гл. VI, § 2, n° 5.)

в) Показать, что если эндоморфизм u нормален, то U является наименьшим выпуклым множеством, содержащим все собственные значения эндоморфизма u. Привести пример, в котором эндоморфизм u не нормален, но множество U обладает указанным свойством. (Взять элементы $\pm 1 \pm i$ в качестве простых собственных значений эндоморфизма u и 0 — как двойное собственное значение.)

*17) Пусть выполнены условия, указанные в n° 3; обозначим через $|\xi|$, $\xi \in A$, элемент $\varrho \geqslant 0$ поля K такой, что $\varrho^2 = \xi\bar{\xi}$ (абсолютное значение элемента ξ). Для всякой квадратной матрицы $M = (\alpha_{ij})$ над полем A положим $f(M) = \max_i \alpha_{ii}$, $g(M) = \max_{i,j} |\alpha_{ij}|$ и обозначим через $\varphi(M)$ наибольшее абсолютное значение собственных значений матрицы M. (Показать, что это определение имеет смысл в случае, когда есть тело кватернионов над полем K.)

а) Пусть A, B, D — квадратные матрицы порядка n над полем A. Показать, что если D диагональна, то

$$g^2(ADB^*) \leqslant f^2(D)\, f(AA^*)\, f(BB^*) \tag{1}$$

(применить неравенство (1) n°1); вывести отсюда, что

$$g(ABB^*A^*) \leqslant f(AA^*)\, \varphi(BB^*) \tag{2}$$

(применить предложение 5 к эрмитовой матрице BB^*). Вывести отсюда, что для m произвольных квадратных матриц A_i $(1 \leqslant i \leqslant m)$ выполняются неравенства:

$$g^2(A_1A_2\ldots A_m) \leqslant f(A_1A_1^*)\, \varphi(A_2A_2^*)\ldots\varphi(A_{m-1}A_{m-1}^*)\, f(A_m^*A_m), \tag{3}$$

$$\varphi^2(A_1A_2\ldots A_m) \leqslant \varphi(A_1A_1^*)\, \varphi(A_2A_2^*)\ldots\varphi(A_mA_m^*), \tag{4}$$

$$g^2(A_1A_2\ldots A_m) \leqslant \varphi(A_1A_1^*)\ldots\varphi(A_mA_m^*) \tag{5}$$

(для доказательства (3) провести индукцию на основе (2); для (4) применить упражнение 12; наконец, из (3) получить (5)).

Показать, что неравенство (3) не обязательно выполняется, если заменить в нем $A_m^*A_m$ на $A_mA_m^*$ (заметить, что возможно неравенство $f(A^*A) \neq f(AA^*)$) или заменить $\varphi(A_iA_i^*)$ на $f(A_iA_i^*)$ для $2 \leqslant i \leqslant m-1$ (взять все A_i равными одной и той же квадратной матрице, все элементы которой равны 1).

б) Пусть u — нормальный эндоморфизм пространства E, λ — его собственное значение (в случае, когда $A=K$, λ — элемент поля $K(i)$); тогда $\lambda\bar{\lambda}$ — собственное значение эндоморфизма u^*u. Для всякой *нормальной* матрицы M (то есть матрицы нормального эндоморфизма пространства E относительно ортонормального базиса) справедливо равенство $\varphi^2(M) = \varphi(MM^*)$. Вывести отсюда, что выполняется неравенство $g(M) \leqslant \varphi(M)$, или, в более общем виде, если матрицы $M_1, \ldots, M_m$ нормальны, то

$$g(M_1\ldots M_m) \leqslant \varphi(M_1)\ldots\varphi(M_m), \tag{6}$$

$$\varphi(M_1\ldots M_m) \leqslant \varphi(M_1)\ldots\varphi(M_m) \tag{7}$$

(применить (4) и (5)).

в) Показать, что для любой положительной эрмитовой матрицы H над полем A выполняются соотношения $f(H) = g(H) \leqslant \varphi(H)$ (записав H в виде AA^*, применить (3) и б)).

18) Пусть выполнены условия, указанные в n° 3.

а) Пусть u — эндоморфизм пространства E, (e_i) — ортонормальный базис, составленный из собственных векторов эндоморфизма u, и ϱ_i — собственное значение эндоморфизма uu^*, соответствующее вектору e_i; положим $s(u) = \left(\sum_{i=1}^{n} \varrho_i\right)^{1/2}$ (если A коммутативно, то это есть квадратный корень из $\mathrm{Tr}(u^*u)$); тогда $s(u^*) = s(u)$. Пусть U и V — матрицы эндоморфизмов u и v пространства E относительно некоторого ортонормального базиса. Показать, что матрица $UV^* + VU^*$

с элементами из поля K удовлетворяет неравенству $(\mathrm{Tr}\,(UV^* + VU^*))^2 \leqslant 4s(u)\,s(v)$ (заметить, что эндоморфизм $(u^* + \lambda v^*)(u + \lambda v)$ положительный эрмитов при любом $\lambda \in K$); вывести отсюда, что $s(u+v) \leqslant s(u) + s(v)$. Если, кроме того, A коммутативно, то

$$|\mathrm{Tr}\,(uv)|^2 \leqslant s(u)\,s(v) \qquad \text{и} \qquad |\mathrm{Tr}\,(u)| \leqslant \sqrt{n}\,s(u)$$

(пользуясь упражнением 14б), записать u как произведение).

б) Предположим дополнительно, что A коммутативно (то есть равно K или $K(i)$). Показать, что для любых положительных эрмитовых квадратных матриц H_1 и H_2 выполняется неравенство $\mathrm{Tr}\,(H_1H_2) > 0$ (свести доказательство к случаю, когда матрица H_2 диагональна). Вывести отсюда, что

$$|\mathrm{Tr}\,(H_1H_2)| \leqslant \varphi(H_1)\,\mathrm{Tr}\,(H_2) \leqslant \mathrm{Tr}\,(H_1)\,\mathrm{Tr}\,(H_2)$$

(обозначения из упражнения 17). Из этих неравенств получить, что для любых двух эндоморфизмов u, v пространства E выполняется неравенство $s(uv) \leqslant s(u)\,s(v)$.

в) Сохраним предположение о коммутативности A. Пусть $\prod_{i=1}^{n}(x - \lambda_i)$ — разложение на линейные множители характеристического многочлена некоторого эндоморфизма u пространства E. Доказать неравенство $\sum_{i=1}^{n} |\lambda_i|^2 \leqslant (s(u))^2$; показать также, что левая и правая части этого неравенства равны тогда и только тогда, когда эндоморфизм u нормален (использовать упражнение 12).

19) Предположим, что выполнены условия из n° 3. Пусть M — квадратная матрица порядка n над телом A; показать, что для всякой ее квадратной подматрицы N (полученной вычеркиванием некоторого числа строк и столбцов с *одинаковыми* номерами) выполняется неравенство $\varphi^2(N) \leqslant \varphi(MM^*)$ (обозначения из упражнения 17) (применить должным образом формулу (4) упражнения 17). Если, в частности, матрица M нормальна, то $\varphi(N) \leqslant \varphi(M)$ (см. упражнение 17в)).

20) Пусть выполнены условия, указанные в n° 3. Предположим дополнительно, что A есть K или $K(i)$. Применить результаты упражнений 17 и 19 к продолжению формы Ф на p-е внешние степени (§ 1, n° 9) и к p-м внешним степеням рассматриваемых матриц и эндоморфизмов. Показать, в частности, что если $\prod_{i=1}^{n}(X - \lambda_i)$ и $\prod_{i=1}^{n}(X - \varrho_i^2)$ — разложения на линейные множители характеристических многочленов эндоморфизма u и эндоморфизма u^*u, причем $|\lambda_i| \geqslant |\lambda_{i+1}|$ и $\varrho_i \geqslant \varrho_{i+1} \geqslant 0$ $(1 \leqslant i \leqslant n-1)$, то при $1 \leqslant n \leqslant n-1$

$$|\lambda_1\lambda_2\ldots\lambda_n| \leqslant \varrho_1\varrho_2\ldots\varrho_n$$

и

$$|\lambda_1\lambda_2\ldots\lambda_n| = \varrho_1\varrho_2\ldots\varrho_n.$$

21) Пусть выполнены условия, указанные в n° 3, u — эрмитов эндоморфизм пространства E и $\prod_{i=1}^{n}(X-\lambda_i)$ — разложение его характеристического многочлена на линейные множители; предположим, что $\lambda_i \geqslant \lambda_{i+1}$ $(1 \leqslant i \leqslant n-1)$.

а) Показать, что наибольшее (соответственно наименьшее) собственное значение λ_i из поля K равно наибольшему (соответственно наименьшему) значению формы $\Phi(u(x), x)$, когда x пробегает множество векторов $x \in E$ таких, что $\Phi(x, x) = 1$. (Доказывать непосредственно или сведя доказательство к случаю $A = K(i)$, применить упражнение 16в) § 7 и упражнение 4 § 3).)

б) Пусть Ψ_V — сужение эрмитовой формы Ψ, ассоциированной с эндоморфизмом u, на векторное подпространство V пространства E, и u_V — эрмитов эндоморфизм подпространства V, ассоциированный с формой Ψ_V. Показать, что если V пробегает множество подпространств пространства E размерности $n-k+1$, то λ_k является наименьшим из наибольших собственных значений эндоморфизмов u_V (использовать предложение 5).

22) Пусть выполнены условия, указанные в n° 3; предположим дополнительно, что A есть $K(i)$ или тело кватернионов над полем K. Пусть u, v — нормальные эндоморфизмы пространства E; пусть, далее, $(E_i)_{1\leqslant i\leqslant r}$ (соответственно $(F_j)_{1\leqslant j\leqslant s}$) — разложение пространства E в прямую сумму попарно ортогональных подпространств таких, что в каждом E_i (соответственно F_j) имеется ортонормальный базис, составленный из собственных векторов эндоморфизма u (соответственно v), соответствующих одному и тому же собственному значению λ_i (соответственно μ_j), причем элементы λ_h и λ_i (соответственно μ_j и μ_k) при $h \neq i$ (соответственно при $j \neq k$) не могут быть переведены друг в друга никаким внутренним автоморфизмом тела A (см. предложение 4 и упражнение 9). Эндоморфизм w пространства E обладает свойством $uw = wv$ тогда и только тогда, когда при любом j $(1 \leqslant j \leqslant s)$ подпространство $w(F_j)$ содержится в одном из E_i и образ всякого собственного вектора эндоморфизма v, соответствующего собственному значению μ_j, при эндоморфизме w есть собственный вектор эндоморфизма u, соответствующий собственному значению μ_j (отсюда, в частности, следует, что элементы μ_j и λ_i переводятся друг в друга некоторым внутренним автоморфизмом тела A). Вывести отсюда, что в этом случае $u^*w = wv^*$.

23) Пусть выполнены условия, указанные в n° 3, и u, v — эндоморфизмы пространства E.

а) Предположим, что эндоморфизмы u и uv нормальны. Показать, что эндоморфизм vu нормален тогда и только тогда, когда u^*u и v перестановочны. (Для доказательства необходимости использовать упражнение 22 и соотношение $u(vu) = (uv)u$; для доказательства достаточности использовать упражнения 14а) и 10г).)

б) Предположим, что эндоморфизмы u, v и uv нормальны; пусть β — наибольшее собственное значение эндоморфизма uu^*, и F — подпространство в E, состоящее из собственных векторов этого эндоморфизма, соответствующих собственному значению β.

Показать, что $v(F) \subset F$. (Заметить, что всякий нормальный эндоморфизм u обладает свойством

$$\Phi(u(x), u(x)) = \Phi(u^*(x), u^*(x))$$

для всех $x \in E$. Свести доказательство к случаю, когда A есть $K(i)$ или тело кватернионов над полем K; подпространство F имеет базис, составленный из собственных векторов эндоморфизма u (и u^*); заметить, что для всякого такого вектора z выполняется равенство $\Phi(u^*uv(z), v(z)) = \beta\Phi(v(z), v(z))$.) Вывести отсюда, что эндоморфизм vu нормален (применить индукцию по числу различных собственных значений эндоморфизма u^*u). Пусть h (соответственно h') — положительный эрмитов эндоморфизм такой, что $h^2 = uu^*$ (соответственно $h'^2 = vv^*$); положим $u = hu_1$, $v = h'v_1$, где u_1 и v_1 — унитарные эндоморфизмы и h перестановочен с u_1, h' перестановочен с v_1 (упражнение 14а)); показать, что пары (h, h'), (h, v_1) и (h', u_1) перестановочны; доказать обратное утверждение. Вывести отсюда, что при этих условиях эндоморфизмы $u^m v^n$, $v^n u^m$, uv^* и v^*u нормальны (m и n — произвольные целые числа > 0).

24) Пусть выполнены условия, указанные в n° 3. Пусть Γ — некоторая группа автоморфизмов пространства E такая, что всякий автоморфизм $u \in \Gamma$ нормален. Показать, что пространство E может быть разложено в прямую сумму попарно ортогональных подпространств E_k $(1 \leqslant k \leqslant r)$ таких, что сужение всякого автоморфизма $u \in \Gamma$ на E_k имеет вид $\lambda_k v_k$, где $\lambda_k > 0$ — элемент поля K, v_k — унитарный эндоморфизм подпространства E_k (каждый элемент $u \in \Gamma$ представить в виде hv, где эндоморфизм v унитарный, эндоморфизм h положительный эрмитов и $h^2 = uu^*$ (упражнение 14а)); воспользоваться упражнением 23б) и применить следствие 2 теоремы 2 к алгебре, порожденной эрмитовыми эндоморфизмами h, соответствующими элементам $u \in \Gamma$). Вывести отсюда, что если группа Γ конечна, то все ее элементы унитарны.

25) Пусть $A = K$ (максимальное упорядоченное поле), L — евклидово пространство размерности n над полем A, имеющее невырожденную положительную метрическую форму.

Пусть S — невырожденная аффинная квадрика в пространстве L (§ 6, упражнение 25). Показать, что если квадрика S имеет центр и этот центр принят за начало в пространстве L, то в L существует ортонормальный базис (e_i), относительно которого квадрика S имеет уравнение $\lambda_1\xi_1^2 + \ldots + \lambda_n\xi_n^2 = 1$. При этом, если два ортонормальных базиса обладают этим свойством, то соответствующие им элементы $\lambda_i \in K$ с точностью до порядка совпадают.

Если квадрика S не имеет центра, то показать, что существует точка $b \in S$ такая, что если b принять за начало, то в пространстве L найдется ортонормальный базис, относительно которого квадрика S имеет уравнение $\lambda_1\xi_1^2 + \ldots \lambda_{n-1}\xi_{n-1}^2 + \ldots + \xi_n = 0$. (Пусть $\overline{S}$ — проективная квадрика такая, что $S = L \cap \overline{S}$, c — (бесконечно удаленный) полюс бесконечно удаленной гиперплоскости H_0 (относительно $\overline{S}$); определить b с помощью условия, что прямая, проходящая через b и c, перпендикулярна к гиперплоскости, касательной к S в точке b.)

*26) а) Пусть K — поле и S — такое его подмножество, что K — максимальное S-упорядочиваемое поле (гл. VI, § 2, упражнение 8). Пусть f — многочлен из кольца $K[X]$, L — его поле корней. Предположим, что для всякой структуры (совершенного) порядка на поле K, согласованной с его структурой кольца, поле L может быть наделено структурой упорядоченного расширения поля K. Показать, что $L = K$ (рассуждать от противного: поступая, как в упражнении 8д), гл. VI, § 2, свести доказательство к случаю, когда $[L : K] = 2$. В заключение заметить, что если элемент $b \in K$ не является квадратом, то существует структура совершенного порядка на поле K, согласованная с его структурой кольца, в которой $b < 0$ (см. гл. VI, § 2, n° 3, лемма к теореме 1)).

б) Перенести результаты n° 3 (за исключением предложения 6) на случай, когда K — максимальное S-упорядочиваемое поле *). (Используя а), доказать сначала утверждение, аналогичное предложению 5. Затем, используя предложение 10, гл. VIII, § 9, n° 4, доказать утверждение, аналогичное следствие 2 теоремы 2, в случае, когда коммутативная алгебра B состоит из эрмитовых эндоморфизмов. При $A = K(i)$ рассмотреть нормальный эндоморфизм u, заметив, что его можно представить в виде $u = v + iw$, где эрмитовы эндоморфизмы u и w перестановочны. Наконец, если A есть тело кватернионов над полем K, рассмотреть пространство E как векторное пространство размерности $2n$ над полем $K(i)$ и, положив $\Phi(x, y) = \Phi_1(x, y) + \Phi_2(x, y)j$, где Φ_1 и Φ_2 принимают значения в $K(i)$, заметить, что если эндоморфизм u нормален относительно Φ, то он нормален и относительно Φ_1.)

*27) Пусть K — максимальное упорядоченное поле, E — векторное пространство размерности n над полем K, Φ — невырожденная симметрическая билинейная форма на пространстве E, сигнатура которой (s, t) отлична от $(n, 0)$ и $(0, n)$. Пусть (e_i) — ортогональный относительно Φ базис, такой, что $\Phi(e_i, e_i) = 1$, $1 \leqslant i \leqslant s$, $\Phi(e_i, e_i) = -1$, $s + 1 \leqslant i \leqslant n$. Для всякого ортогонального преобразования $u \in U(\Phi)$ запишем его матрицу относительно базиса (e_i) в виде

*) Эти (неопубликованные) результаты сообщены нам И. Капланским.

таблицы

$$U=\begin{pmatrix} M & N \\ P & Q \end{pmatrix}$$

из матриц, соответствующих разбиению отрезка $[1, n]$ на $[1, s]$ и $[s+1, n]$.

а) Доказать равенства

$$^tM\cdot M-{}^tP\cdot P=I_s,$$
$$^tQ\cdot Q-{}^tN\cdot N=I_t,$$
$$^tM\cdot N-{}^tP\cdot Q=0.$$

б) Пусть R — матрица над полем K, имеющая t строк и s столбцов, такая, что $I_s-{}^tR\cdot R$ является матрицей невырожденной положительной эрмитовой формы (над K^s). Показать, что $\det(M+\lambda NR)$ не меняет знака при $-1\leqslant\lambda\leqslant 1$ в поле K (используя а), показать, что $^t(M+\lambda NR)(M+\lambda NR)$ является матрицей невырожденной положительной симметрической формы).

в) Положим $\sigma(u)=\sigma(U)=\operatorname{sgn}(\det M)$; показать, что для любых элементов u, v ортогональной группы $U(\Phi)$ выполняется равенство $\sigma(uv)=\sigma(u)\,\sigma(v)$ (использовать а) и б)). Вывести отсюда, что коммутант специальной ортогональной группы $\boldsymbol{SU}(\Phi)$ отличен от $\boldsymbol{SU}(\Phi)$ (см. § 10, упражнение 9).

§ 8. Типы квадратичных форм

В этом параграфе предполагается, что A — поле.

1. Типы квадратичных форм

Если на векторном пространстве E над полем A задана квадратичная форма Q (§ 3, n° 4), то E называют *пространством определения* формы Q, а $\dim(E)$ — *размерностью формы* Q. Для двух квадратичных форм Q и Q', заданных на пространствах E и E' над полем A, через $Q\top Q'$ будем обозначать их прямую сумму (§ 3, n° 4). Напомним, что прямая сумма нейтральных форм является нейтральной формой (§ 4, n° 2).

Введем следующее отношение:

«Q и Q' — невырожденные квадратичные формы конечной размерности над полем A, и существуют нейтральные квадратичные формы N и N' такие, что форма $Q\top N$ эквивалентна $Q'\top N'$».

Ясно, что это отношение, обозначаемое в дальнейшем $Q\sim Q'$, рефлексивно и симметрично. В то же время оно транзитивно: в самом деле, если для трех квадратичных форм Q, Q' и Q'' выпол-

нены условия $Q \sim Q'$ и $Q' \sim Q''$, то существуют нейтральные формы M, M', N, N' такие, что форма $Q \perp M$ эквивалентна $Q' \perp M'$, а $Q' \perp N$ эквивалентна $Q'' \perp N'$; тогда форма $Q \perp (M \perp N)$ эквивалентна $(Q \perp M) \perp N$ и, следовательно, форме $(Q' \perp M') \perp N$; точно так же она эквивалентна $(Q' \perp N) \perp M'$, то есть $(Q'' \perp N') \perp M'$ и $Q'' \perp (N' \perp M')$; так как формы $M \perp N$ и $N' \perp M'$ нейтральны, то $Q \sim Q''$. Таким образом, отношение $Q \sim Q'$ является *отношением эквивалентности* между Q и Q'. Ясно, что если две невырожденные квадратичные формы Q и Q' конечной размерности эквивалентны, то $Q \sim Q'$.

Для всякой невырожденной конечномерной формы Q над полем A положим

$$\vartheta(Q) = \tau_X(X \sim Q), \tag{1}$$

$\vartheta(Q)$ будем называть *типом* формы Q. Для любых двух конечномерных невырожденных форм над полем A соотношения $Q \sim Q'$ и $\vartheta(Q) = \vartheta(Q')$ эквивалентны.

Предложение 1. *Пусть Q и Q' — невырожденные конечномерные формы над полем A. Для того чтобы формы Q и Q' были эквивалентны, необходимо и достаточно, чтобы они были одного типа и имели одинаковую размерность.*

Необходимость этого условия очевидна. Предположим, что оно выполнено. Тогда существуют нейтральные формы N и N' такие, что формы $Q \perp N$ и $Q' \perp N'$ эквивалентны. Поскольку последние две формы имеют одинаковую размерность, то N и N' также имеют одинаковую размерность и, следовательно, эквивалентны (§ 4, n° 2, следствие 2 предложения 2). Поэтому вследствие теоремы Витта (§ 4, n° 3, следствие 1 теоремы 1) формы Q и Q' эквивалентны.

Предложение 2. *Отношение «существует невырожденная конечномерная квадратичная форма Q над полем A такая, что $X = \vartheta(Q)$» является коллективизирующим по X* (Теор. мн., гл. II, § 1, n° 4).

В самом деле, пусть V — бесконечномерное пространство над полем A, $\mathfrak{S}$ — множество невырожденных квадратичных форм на конечномерных подпространствах пространства V, и $\mathfrak{M}$ — множество типов $\vartheta(Q)$ квадратичных форм $Q \in \mathfrak{S}$. Ясно, что

всякая невырожденная конечномерная квадратичная форма Q' над полем A эквивалентна по крайней мере одной форме из множества $\mathfrak{S}$; поэтому $\vartheta(Q') \in \mathfrak{M}$, что и требовалось доказать

2. *Группа типов квадратичных форм*

Наделим множество $\mathfrak{M}$ типов конечномерных невырожденных квадратичных форм над полем A структурой *коммутативной группы*. Определим во множестве $\mathfrak{M}$ сложение следующей формулой:

$$T + T' = \vartheta(T \top T') \qquad (T, T' \in \mathfrak{M}). \tag{2}$$

Это сложение коммутативно, так как форма $T' \top T$ эквивалентна $T \top T'$, и ассоциативно, так как для любых элементов T, T', T'' множества $\mathfrak{M}$ выполняются соотношения

$$(T + T') + T'' \sim (T + T'') \top T' \sim (T \top T') \top T'' \sim$$
$$\sim T \top (T' \top T'') \sim T \top (T' + T'') \sim T + (T' + T''),$$

откуда $(T + T') + T'' = T + (T' + T'')$, так как два элемента одного типа из множества $\mathfrak{M}$ равны. Кроме того, определенное выше сложение обладает нейтральным элементом: ясно, что все нейтральные формы имеют один и тот же тип T_0, являющийся типом нулевой формы размерности нуль; легко видеть, что тип T_0 является искомым нейтральным элементом. Наконец, существование противоположного элемента для любого $T \in \mathfrak{M}$ сразу следует из предложения:

Предложение 3. *Пусть Q — конечномерная невырожденная квадратичная форма на векторном пространстве V над полем A. Определим форму $-Q$ на пространстве V формулой $(-Q)(x) = -Q(x)$ $(x \in V)$. Тогда форма $Q \top (-Q)$ нейтральна.*

В самом деле, сужение формы $Q \top (-Q)$ на диагональ D произведения $V \times V$ равно нулю. Следовательно, индекс этой формы $\geqslant \frac{1}{2} \dim (V \times V)$ (§ 4, n° 2, определение 3) и по формуле (4) равен $\frac{1}{2} \dim (V \times V)$ (там же). Отсюда следует, что форма $Q \top (-Q)$ нейтральна (там же).

Это позволяет ввести следующее определение:

Определение 1. *Множество типов конечномерных невырожденных форм над полем A, наделенное сложением по формуле* (2), *называется группой типов квадратичных форм или группой Витта поля A.*

Замечания. 1) Всякая конечномерная невырожденная форма Q нулевого типа (то есть форма, для которой в наших обозначениях $\vartheta(Q) = T_0$) является нейтральной. В самом деле, существуют нейтральные формы N и N' такие, что форма $Q \perp N$ эквивалентна N'. Следовательно, форма Q имеет четную размерность, так что существует нейтральная форма N_1 той же размерности, что и Q. Поскольку формы Q и N_1 одного типа, из предложения 1 следует, что они эквивалентны. Таким образом, форма Q нейтральна.

2) Пусть $\delta(Q)$ — класс по модулю 2 размерности произвольной конечномерной квадратичной формы Q над полем A. Тогда, поскольку всякая нейтральная форма N имеет четную размерность, $\delta(N) = 0$; следовательно, если $Q \sim Q'$, то $\delta(Q) = \delta(Q')$. Таким образом, сужение δ на группу $\mathfrak{M}$ типов квадратичных форм является гомоморфизмом группы $\mathfrak{M}$ в группу $\boldsymbol{Z}/(2)$. Этот гомоморфизм сюръективен в случае, когда характеристика поля A не равна 2, но не сюръективен, если A имеет характеристику 2, так как в этом случае всякая квадратичная форма нечетной размерности вырождена, поскольку ассоциированная с ней билинейная форма знакопеременна (см. § 5).

3) Пусть $a \neq 0$ — элемент поля A. Если форма N нейтральна, то форма aN также нейтральна. Отсюда ясно, что если $Q \sim Q'$, то и $aQ \sim aQ'$. Для всякого элемента T группы $\mathfrak{M}$ положим

$$a \cdot T = \vartheta(aT). \tag{3}$$

Тем самым мы получаем внешний закон композиции между группой A^* ненулевых элементов поля A и группой $\mathfrak{M}$. Справедливость следующих формул вытекает непосредственно из определения

$$a \cdot (T + T') = a \cdot T + a \cdot T', \qquad ab \cdot T = a \cdot (b \cdot T) \tag{4}$$
$$(a, b \in A^*,\ T, T' \in \mathfrak{M}).$$

Однако если a, b и $a + b$ входят в A^*, то равенство $(a + b) \cdot T = a \cdot T + b \cdot T$, вообще говоря, неверно.

Предложение 4. *Пусть Q — невырожденная квадратичная форма на векторном пространстве E конечной размерности над полем A. Предположим, что характеристика поля A не равна 2, и пусть $(x_1, \ldots, x_n)$ — ортогональный базис пространства V. Обозначим через T_1 тип квадратичной формы Q_1, определенной на векторном пространстве A и такой, что $Q_1(1) = 1$. Тогда тип формы Q равен $\sum_{i=1}^{n} Q(x_i) \cdot T_1$.*

В самом деле, форма Q эквивалентна сумме

$$(Q(x_1)Q_1)\top\ldots\top(Q(x_n)Q_n).$$

Следствие. *В обозначениях и предположениях предложения* 3 *множество элементов вида* $a\cdot T_1$ ($a\in A^*$) *составляет множество образующих группы типов квадратичных форм над полем* A.

Таким образом, исследование структуры группы типов квадратичных форм над полем A сводится к исследованию $\boldsymbol{Z}$-линейных соотношений между элементами вида $a\cdot T_1$. Если $b\in A^*$, то форма Q_1, определенная в предложении 4, очевидно, эквивалентна b^2Q_1; отсюда $a\cdot T_1 = ab^2\cdot T_1$, так что элемент $a\cdot T_1$ зависит только от класса элемента a по модулю подгруппы $(A^*)^2$ квадратов элементов группы A^*. Кроме того, из предложения 3 следует равенство $(-a)\cdot T_1 = -a\cdot T_1$. Однако между элементами $a\cdot T_1$, вообще говоря, существуют еще и другие $\boldsymbol{Z}$-линейные соотношения, кроме тех, которые выводятся из соотношений, только что указанных.

Предложение 5. *Пусть* A — *максимальное упорядоченное поле,* Q — *конечномерная невырожденная квадратичная форма над полем* A *и* (s, t) — *ее сигнатура* (§ 7, n° 2, определение 2). *Тогда тип формы* Q *есть* $(s-t)\cdot T_1$ *и группа* $\mathfrak{M}$ *типов квадратичных форм над полем* A *является бесконечной моногенной группой, порожденной типом* T_1.

В самом деле, факторгруппа $A^*/(A^*)^2$ имеет порядок 2 и $(-1)\cdot T_1 = -T_1$, так что группа $\mathfrak{M}$ порождается типом T_1, то есть моногенна. Для любого $n>0$ $n\cdot T_1$ является типом положительных невырожденных квадратичных форм размерности n; поскольку эти формы не являются нейтральными, $n\cdot T_1\neq 0$, то есть группа $\mathfrak{M}$ бесконечна. Наконец, форма с сигнатурой (s, t) изоморфна прямой сумме s форм Q_1 (в обозначениях предложения 4) и t форм $-Q_1$ (§ 7, n° 2, теорема 1); отсюда следует, что ее тип равен $(s-t)\cdot T_1$.

3. Кольцо типов квадратичных форм

В этом n° предполагается, что A — поле *характеристики* $\neq 2$.

Пусть Q и Q' — квадратичные формы на векторных пространствах V и V' над полем A. Тензорным произведением форм Q и Q' назовем такую квадратичную форму $Q\otimes Q'$ на произведении

$V \otimes V'$, у которой ассоциированная билинейная форма является тензорным произведением (§ 1, n° 9, определение 11) билинейных форм, ассоциированных с формами Q и Q'. Легко видеть, что форма $Q \otimes Q'$ удовлетворяет соотношению

$$(Q \otimes Q')(x \otimes x') = Q(x)\,Q(x') \qquad (x \in V,\ x' \in V'). \tag{5}$$

Если обе формы Q и Q' конечномерны и невырождены, то их тензорное произведение $Q \otimes Q'$ также конечномерно и невырождено (§ 1, n° 9, предложение 9).

Пусть Q, Q', Q'' — квадратичные формы на векторных пространствах V, V', V''. Используя канонический изоморфизм произведения $V \otimes V'$ на $V' \otimes V$ (соответственно $(V \otimes V') \otimes V''$ на $V \otimes (V' \otimes V'')$, $(V \times V') \otimes V''$ на $(V \otimes V'') \times (V' \otimes V'')$), легко показать, что форма $Q \otimes Q'$ эквивалентна $Q' \otimes Q$ (соответственно $(Q \otimes Q') \otimes Q''$ эквивалентна $Q \otimes (Q' \otimes Q'')$, $(Q \perp Q') \otimes Q''$ эквивалентна $(Q \otimes Q'') \perp (Q' \otimes Q'')$).

Пусть Q и Q' — конечномерные невырожденные квадратичные формы. Если форма Q *нейтральна*, то и $Q \otimes Q'$ нейтральна. В самом деле, пусть V и V' — пространства определения форм Q и Q', $2n$ и n' — размерности V и V', W — вполне сингулярное подпространство размерности n пространства V (§ 4, n° 2); тогда подпространство $W \otimes V'$ вполне сингулярно и его размерность равна половине размерности пространства $V \otimes V'$; отсюда так же, как и в предложении 3, следует, что форма $Q \otimes Q'$ нейтральна. Аналогично форма $Q \otimes Q'$ будет нейтральной, если нейтральна форма Q'.

Отсюда следует, что если Q, Q', Q_1, Q'_1 — конечномерные невырожденные квадратичные формы над полем A и $\vartheta(Q_1) = \vartheta(Q)$ и $\vartheta(Q'_1) = \vartheta(Q')$, то $\vartheta(Q_1 \otimes Q'_1) = \vartheta(Q \otimes Q')$. В самом деле, достаточно проверить это равенство в случае, когда $Q_1 = Q \perp N$ и $Q'_1 = Q' \perp N'$, где N и N' — нейтральные формы; тогда форма $Q_1 \otimes Q'_1$ эквивалентна форме

$$(Q \otimes Q') \perp (Q \otimes N' \perp Q' \otimes N \perp N \otimes Q');$$

во второй скобке здесь стоит нейтральная форма, так что наше утверждение доказано.

Пусть теперь $\mathfrak{M}$ — группа типов квадратичных форм над полем A. Определим на множестве $\mathfrak{M}$ второй закон композиции,

записываемый мультипликативно, формулой

$$TT' = \vartheta(T \otimes T') \quad (T, T' \in \mathfrak{M}). \tag{6}$$

Из предыдущих рассуждений легко следует, что этот закон композиции коммутативен, ассоциативен и дистрибутивен относительно сложения. Он имеет единицу, именно, тип T_1 квадратичной формы Q_1, определенной на пространстве A и такой, что $Q_1(1) = 1$; в самом деле, по формуле (5) $Q_1 \otimes Q = Q$ для любой квадратичной формы Q. Таким образом, аддитивная группа $\mathfrak{M}$, наделенная только что определенным умножением, будет коммутативным кольцом с единицей; это кольцо называется *кольцом типов квадратичных форм* поля A (или, если не может возникнуть недоразумения, *кольцом Витта* поля A).

Замечания. 1) Ясно, что для любого элемента $a \in A^*$ и любых элементов T и T' группы $\mathfrak{M}$ выполняются равенства

$$a \cdot (TT') = (a \cdot T)\, T' = T\,(a \cdot T'). \tag{7}$$

Заметим, кроме того, что $a \cdot T = T_a T$, где T_a — тип квадратичной формы aQ_1 над полем A.

2) Поскольку поле A имеет характеристику $\neq 2$, всякий элемент $T \in \mathfrak{M}$ имеет вид $\sum_{i=1}^{n} a_i \cdot T_1$, где $a_i \in A^*$ (n° 2, предложение 4), и

$$\Big(\sum_{i=1}^{n} a_i \cdot T_1\Big)\Big(\sum_{j=1}^{q} b_j \cdot T_1\Big) = \sum_{i,\,j} a_i b_j \cdot T_1) \qquad (a,\ b \in A^*). \tag{8}$$

3) Пусть A — *максимальное упорядоченное поле*. Тогда кольцо $\mathfrak{M}$ изоморфно $\boldsymbol{Z}$ (предложение 5) (типу квадратичной формы с сигнатурой (s, t) поставить в соответствие число $s - t$ (там же)). Так как тензорное произведение двух форм Q и Q' с сигнатурами (s, t) и (s', t') является формой размерности $(s + t)(s' + t')$, то отсюда с помощью элементарного подсчета следует, что сигнатура формы $Q \otimes Q'$ равна $(ss' + tt',\ st' + ts')$.

§ 9. Алгебры Клиффорда

В этом параграфе кольцо A предполагается коммутативным. Q — квадратичная форма на A-модуле E, Φ — ассоциированная с Q билинейная форма (§ 3, n° 4).

1. Определение и универсальное свойство алгебры Клиффорда

Определение 1. *Алгеброй Клиффорда формы Q называется факторалгебра $C(Q)$ тензорной алгебры $T(E)$ модуля E по двустороннему идеалу $I(Q)$, порожденному элементами вида $x \otimes x - Q(x) \cdot 1$ $(x \in E)$.*

Обозначим через ϱ_Q (или просто ϱ, если не может возникнуть недоразумения) отображение модуля E в $C(Q)$, являющееся композицией канонического отображения модуля E в $T(E)$ и канонического отображения $T(E)$ на $C(Q)$; отображение ϱ_Q называется *каноническим*. Заметим, что алгебра $C(Q)$ порождается образом $\varrho_Q(E)$ и для $x \in E$

$$\varrho(x)^2 = Q(x) \cdot 1, \tag{1}$$

откуда, заменяя x на $x+y$ $(x,\ y \in E)$, получим

$$\varrho(x)\varrho(y) + \varrho(y)\varrho(x) = \Phi(x, y) \cdot 1. \tag{2}$$

Пример. Если модуль e имеет базис из единственного элемента e, то алгебра $T(E)$ изоморфна алгебре многочленов $A[X]$ и $C(Q)$ является квадратичным расширением кольца A и имеет базис $(1, u)$, где $u = \varrho(e)$ и $u^2 = Q(e)$.

Пусть T^h — h-я тензорная степень $\overset{h}{\otimes} E$ в алгебре $T(E)$ и T^+ (соответственно T^-) — сумма всех T^h с четными h (соответственно с нечетными h). Поскольку $T(E)$ является прямой суммой T^+ и T^-, а идеал $I(Q)$ порождается элементами из T^+, $I(Q)$ будет прямой суммой пересечений $T^+ \cap I(Q)$ и $T^- \cap I(Q)$, а $C(Q)$ — прямой суммой двух подмодулей $C^+(Q) = \sigma(T^+)$ и $C^-(Q) = \sigma(T^-)$ (эти подмодули обозначаются также C^+ и C^-). Элементы подмодуля C^+ (соответственно C^-) будут называться *четными* (соответственно *нечетными*). Справедливы включения

$$C^+C^+ \subset C^+, \quad C^+C^- \subset C^-, \quad C^-C^+ \subset C^-, \quad C^-C^- \subset C^+. \tag{3}$$

В частности, C^+ является подалгеброй в $C(Q)$.

Предложение 1. *Пусть f — линейное отображение модуля E в алгебру D над полем A такое, что $f(x)^2 = Q(x) \cdot 1$ для любого $x \in E$. Существует единственный гомоморфизм $\bar{f}$ алгебры $C(Q)$ в D, удовлетворяющий условию $f = \bar{f} \circ \varrho_Q$.*

Единственность гомоморфизма $\bar{f}$ следует из того, что алгебра $C(Q)$ порождается образом $\varrho_Q(E)$. Пусть h — единственный гомоморфизм алгебры $T(E)$ в D, продолжающий f (h определяется равенством $h(x_1 \otimes \ldots \otimes x_n) = f(x_1) \ldots f(x_n)$). Тогда

$$h(x \otimes x - Q(x) \cdot 1) = (f(x)^2 - Q(x)) \cdot 1 = 0,$$

и следовательно, гомоморфизм h аннулируется на идеале $I(Q)$ и посредством факторизации определяет искомый гомоморфизм $\bar{f}$.

Предложение 1 показывает, что алгебра $C(Q)$ является решением проблемы универсального отображения (Теор. мн., гл. IV, § 3, n° 1).

Возьмем, в частности, в качестве D алгебру, *противоположную* $C(Q)$, и в качестве f отображение ϱ; вследствие предложения 1 существует единственный антиавтоморфизм β алгебры $C(Q)$, сужение которого на $\varrho(E)$ тождественно; этот антиавтоморфизм называется *главным антиавтоморфизмом* алгебры $C(Q)$. Ясно, что $\beta^2 = 1$.

С другой стороны, пусть Q' — квадратичная форма на A-модуле E' и f — линейное отображение модуля E в E' такое, что $Q' \circ f = Q$. Тогда $\varrho_{Q'}(f(x))^2 = Q'(f(x)) \cdot 1 = Q(x) \cdot 1$, и следовательно, существует единственный гомоморфизм $C(f)$ алгебры $C(Q)$ в $C(Q')$ такой, что $C(f) \circ \varrho_Q = \varrho_{Q'} \circ f$. Если отображение f тождественно, то и $C(f)$ тождественно; если еще заданы квадратичная форма Q'' на A-модуле E'' и линейное отображение g модуля E' в E'' такое, что $Q'' \circ g = Q'$, то $C(g \circ f) = C(g) \circ C(f)$. В случае, когда E' — подмодуль модуля E, а f — каноническая инъекция подмодуля E' в E (откуда следует, что Q' — сужение формы Q на E'), гомоморфизм $C(f)$ называется *каноническим* гомоморфизмом алгебры $C(Q')$ в $C(Q)$.

Возьмем, в частности, $Q' = Q$, а в качестве f отображение $x \to -x$; тогда существует единственный *автоморфизм* α алгебры $C(Q)$ такой, что $\alpha \circ \varrho = -\varrho$; этот автоморфизм называется *главным автоморфизмом* алгебры $C(Q)$. Ясно, что $\alpha^2 = 1$ и что сужение α на C^+ (соответственно C^-) тождественно (естественно, есть $u \to -u$).

Предложение 2. *Пусть A' — коммутативное кольцо, φ — гомоморфизм кольца A в A', Q' — квадратичная форма на $E' = A' \otimes_A E$, получаемая из формы Q расширением скаляров*

(§ 3, n° 4, предложение 3). *Существует единственный автоморфизм j алгебры $A' \otimes_A C(Q)$ на алгебру $C(Q')$ такой, что $j(1 \otimes \varrho_Q(x)) = \varrho_{Q'}(1 \otimes x)$ для любого $x \in E$.*

Достаточно доказать, что алгебра $C' = A' \otimes C(Q)$ и отображение $1 \otimes \varrho_Q$ модуля E' в C' образуют решение той же проблемы универсального отображения, что и алгебра $C(Q')$ и отображение $\varrho_{Q'}$. Пусть D' — алгебра над кольцом A' и f' — A'-линейное отображение модуля E' в D' такое, что $f'(x')^2 = Q'(x') \cdot 1$ для любого $x' \in E'$. Отображение g: $x \to f'(1 \otimes x)$ модуля E в D' (D' рассматривается как A-модуль в соответствии с гомоморфизмом φ) A-линейно, и $g(x)^2 = Q'(1 \otimes x) \cdot 1 = Q(x) \cdot 1$ для любого $x \in E$. Тогда существует единственный A-гомоморфизм $\bar{g}$ алгебры $C(Q)$ в D' такой, что $\bar{g}(\varrho_Q(x)) = f'(1 \otimes x)$. Следовательно, существует единственный A'-гомоморфизм $\bar{f}'$ алгебры C' в D' такой, что $\bar{f}'(1 \otimes \varrho_Q(x)) = f'(1 \otimes x)$ для любого $x \in E$; отсюда по линейности следует равенство $\bar{f}'((1 \otimes \varrho_Q)(x')) = f'(x')$ для любого $x' \in E'$, что и требовалось доказать.

2. *Некоторые операции в тензорной алгебре*

В этом n° e_x ($x \in E$) означает линейное отображение $u \to x \otimes u$ тензорной алгебры $T(E)$ в себя.

Лемма 1. *Пусть f — элемент сопряженного к E модуля E^*. Существует единственное линейное отображение i_f алгебры $T(E)$ в себя, удовлетворяющее условиям:*

$$i_f(1) = 0, \tag{4}$$

$$i_f \circ e_x + e_x \circ i_f = f(x) \cdot I \quad \text{для любого } x \in E \tag{5}$$

(где I — тождественное отображение). Отображение $f \to i_f$ модуля E^* в $\mathscr{L}(T(E))$ линейно. Выполняются соотношения $i_f(T^n) \subset T^{n-1}$, $(i_f)^2 = 0$ и $i_f \circ i_g + i_g \circ i_f = 0$ для всяких f, $g \in E^*$. Отображение i_f равно нулю на подалгебре алгебры $T(E)$, порожденной ядром элемента f. Идеал $I(Q)$ устойчив относительно i_f; следовательно, отображение i_f посредством факторизации определяет линейное отображение алгебры $C(Q)$ в себя (также обозначаемое i_f).

В самом деле, формулу (5) можно записать в виде

$$i_f(x \otimes u) = -x \otimes i_f(u) + f(x) \cdot u \quad (x \in E,\ u \in T(E)). \tag{6}$$

Равенство (4) полностью определяет отображение i_f на T^0, а равенство (6) определяет i_f на T^n, если известны значения отображения i_f на T^{n-1}. Отсюда следует единственность отображения i_f. С другой стороны, для $x \in E$ и $u \in T^{n-1}$ правая часть равенства (6) является билинейным отображением на произведении $E \times T^{n-1}$; отсюда индукцией по n следует существование отображения i_f (гл. III, § 1, n° 2) и, также по индукции, включение $i_f(T^n) \subset T^{n-1}$. Если $f = ag + bh$ $(a, b \in A,\ g, h \in E^*)$, то отображение $ai_g + bi_h$ довлетворяет условиям (4) и (5), то есть равно i_f. Имеем

$$(i_f)^2 \circ e_x = -i_f \circ e_x \circ i_f + f(x)\, i_f = e_x \circ (i_f)^2,$$

откуда индукцией по n, в силу равенства $(i_f)^2(1) = 0$, получаем, что $(i_f)^2 = 0$ на T^n. Заменив f на $f + g$, из равенства $(i_f)^2 = 0$ получим, что $i_f \circ i_g + i_g \circ i_f = 0$. Индукция, аналогичная предыдущей, показывает, что i_f обращается в нуль на подалгебре, порожденной ядром элемента f. Наконец, из равенства (6) следует, что множество элементов $u \in I(Q)$ таких, что $i_f(u) \in I(Q)$, является левым идеалом в алгебре $T(E)$; более того, если $u = (x \otimes x - Q(x)\cdot 1) \otimes v$ $(x \in E,\ v \in T(E))$, то

$$\begin{aligned} i_f(u) &= f(x)\, x \otimes v - x \otimes i_f(x \otimes v) - Q(x)\, i_f(v) = \\ &= f(x)\, x \otimes v - f(x)\, x \otimes v + x \otimes x \otimes i_f(v) - Q(x)\, i_f(v) = \\ &= (x \otimes x - Q(x)\cdot 1) \otimes i_f(v); \end{aligned}$$

следовательно, идеал $I(Q)$ устойчив относительно i_f, откуда следует последнее из доказываемых утверждений.

Пусть F — билинейная форма на модуле E. В оставшейся части параграфа мы будем обозначать через i_x^F $(x \in E)$ отображение i_f, соответствующее линейной форме f: $y \to F(x, y)$ на модуле E.

Лемма 2. *Существует единственное отображение λ_F алгебры $T(E)$ в себя, удовлетворяющее условиям*

$$\lambda_F(1) = 0, \tag{7}$$

$$\lambda_F \circ e_x = (e_x + i_x^F) \circ \lambda_F \qquad (x \in E). \tag{8}$$

Для любого $f \in E^*$ выполняется равенство

$$\lambda_F \circ i_f = i_f \circ \lambda_F. \tag{9}$$

В самом деле, формула (8) означает, что

$$\lambda_F(x \otimes u) = x \otimes \lambda_F(u) + i_x^F(\lambda_F(u)) \qquad (x \in E,\ u \in T(E)). \tag{10}$$

Равенство (7) полностью определяет отображение λ_F на T^0, а равенство (10) определяет λ_F на T^n, если известны его значения на T^{n-1}. Отсюда следует единственность отображения λ_F. С другой стороны, для $x \in E$ и $u \in T^{n-1}$ правая часть равенства (10) является билинейным отображением на произведении $E \times T^{n-1}$; отсюда индукцией по n устанавливается существование отображения λ_F. Остается доказать формулу (9). Мы сделаем это по индукции; обе части равенства (9) равны нулю на T^0; предположим, что (9) верно на $\sum_{h=0}^{n-1} T^h$; тогда для $x \in E$ и $u \in T^{n-1}$ имеем

$$(\lambda_F \circ i_f)(x \otimes u) = (-\lambda_F \circ e_x \circ i_F + f(x)\lambda_F)(u) = -(e_x + i_x^F) \circ \lambda_F \circ i_F(u) +$$
$$+ f(x)\lambda_F(u) = -(e_x + i_x^F) \circ i_f \circ \lambda_F(u) + f(x)\lambda_F(u) =$$
$$= (i_f \circ e_x \circ \lambda_F - f(x)\lambda_F - i_f \circ i_x^F \circ \lambda_F + f(x)\lambda_F)(u) =$$
$$= (i_f \circ (e_x + i_x^F) \circ \lambda_F)(u) = (i_f \circ \lambda_F)(x \otimes u),$$

откуда следует последнее доказываемое утверждение.

Лемма 3. *Пусть F и G — билинейные формы на модуле E. Тогда $\lambda_F \circ \lambda_G = \lambda_{F+G}$. Для всякой билинейной формы F на модуле E отображение λ_F является биекцией алгебры $T(E)$ на себя.*

В самом деле, отображение $\lambda_F \circ \lambda_G$ обладает свойствами (7) и (8), характеризующими отображение λ_{F+G}: $(\lambda_F \circ \lambda_G)(1) = 0$ и

$$\lambda_F \circ \lambda_G \circ e_x = \lambda_F \circ (e_x + i_x^G) \circ \lambda_G = (e_x + i_x^G + i_x^F) \circ \lambda_F \circ \lambda_G =$$
$$= (e_x + i_x^{F+G}) \circ \lambda_F \circ \lambda_G.$$

С другой стороны, если $F = 0$, то $i_x^F = 0$ для любого $x \in E$, и поэтому $\lambda_F = I$, откуда следует, что $\lambda_F \circ \lambda_{-F} = \lambda_{-F} \circ \lambda_F$ для любого F.

3. *Базис алгебры Клиффорда*

Предложение 3. *Пусть Q и Q' — квадратичные формы, F — билинейная форма на модуле E и $Q'(x) = Q(x) + F(x, x)$ для любого $x \in E$. Тогда λ_F отображает идеал $I(Q')$ на идеал $I(Q)$ и определяет изоморфизм (обозначаемый $\overline{\lambda}_F$) A-модуля $C(Q')$ на A-модуль $C(Q)$.*

Так как λ_F — биекция и λ_{-F} — обратная ей биекция (лемма 3), достаточно доказать включение $\lambda_F(I(Q')) \subset I(Q)$. Идеал $I(Q)$ является левым идеалом, устойчивым относительно отображения i_x^F (лемма 1), так что из (8) следует, что множество элементов $u \in T(E)$ таких, что $\lambda_F(u) \in I(Q)$, является левым идеалом. Поэтому достаточно показать, что для любых $u \in T(E)$ и $x \in E$ имеем

$$\lambda_F(x \otimes x \otimes u - Q'(x)\, u) \in I(Q).$$

Но по формуле (8) и лемме 1

$$\lambda_F \circ e_x^2 = (e_x + i_x^F) \circ \lambda_F = (e_x^2 + F(x, x)) \circ \lambda_F,$$

откуда

$$\lambda_F(x \otimes x \otimes u - Q'(x)\, u) = (e_x^2 + F(x, x) - Q'(x)) \circ \lambda_F(u) = \\ = (x \otimes x - Q(x)) \otimes \lambda_F(u) \in I(Q).$$

Лемма 4. *Если квадратичная форма Q равна нулю, то алгебра $C(Q)$ является внешней алгеброй модуля E.*

В самом деле, внешняя алгебра модуля E есть факторалгебра $T(E)$ по двустороннему идеалу J, порожденному элементами $a \otimes v \otimes a$ ($a \in E$, $v \in T(E)$) (гл. III, § 5, n° 5 и n° 9). Ясно, что $I(Q) \subset J$. Достаточно, следовательно, доказать, что $a \otimes v \otimes a \in I(Q)$. Это очевидно, если $v \in T^0$; предположим, что это утверждение доказано для $v \in \sum_{h=0}^{n-1} T^h$, и пусть $x \in E$ и $u \in T^{n-1}$; тогда

$$a \otimes x \otimes u \otimes a = (a + x) \otimes (a + x) \otimes u \otimes a - \\ - a \otimes a \otimes u \otimes a - x \otimes a \otimes u \otimes a - x \otimes x \otimes u \otimes a$$

и все четыре члена в правой части принадлежат идеалу $I(Q)$.

Предположим, в частности, что модуль E имеет *базис* $(x_i)_{i \in L}$, и совершенно упорядочим множество индексов L. Известно (гл. III, § 5, n° 6), что внешняя алгебра модуля E имеет базис, состоящий из элементов x_H, где H пробегает множество конечных подмножеств из L, а x_H имеет вид $x_{h_1} \wedge \ldots \wedge x_{h_q}$, где $(h_1, \ldots, h_q)$ — строго возрастающая последовательность элементов из H.

С другой стороны, рассмотрим билинейную форму F, определяемую равенствами: $F(x_i, x_j) = -\Phi(x_i, x_j)$, если $i > j$, $F(x_i, x_j) = 0$, если $i < j$, и $F(x_i, x_i) = Q(x_i)$. Ясно, что $Q(x) + F(x, x) = 0$; из предложения 3 и леммы 4 следует, что отображение $\overline{\lambda}_F$ (обозначение из предложения 3) будет изоморфизмом модуля $\bigwedge E$ на алгебру $C(Q)$, являющуюся, следовательно, свободным A-модулем. Индукцией по числу элементов множества H докажем равенство

$$\overline{\lambda}_F(x_H) = \varrho(x_{h_1}) \ldots \varrho(x_{h_q}). \tag{11}$$

(где $h_1, \ldots, h_q$ — строго возрастающая последовательность элементов множества H). Если H пусто или содержит один элемент, то это утверждение очевидно. Предположим, что равенство (11) верно для любых подмножеств, содержащих не более чем $q-1$ элементов. Рассмотрим множество H из q элементов. Обозначим через j его наименьший элемент и положим $H = \{j\} \cup K$, где подмножество K имеет $q-1$ элементов. По формуле (8) и предположению индукции имеем

$$\overline{\lambda}_F(x_H) = \overline{\lambda}_F(x_j \wedge x_K) = \varrho(x_j)\,\overline{\lambda}_F(x_K) + i^F_{x_j}(\overline{\lambda}_F(x_K)) = x'_H + i^F_{x_j}(x'_K),$$

где $x'_J = \varrho(x_{j_1}) \ldots \varrho(x_{j_s})$ для любого конечного подмножества J множества H и $(j_1, \ldots, j_s)$ — возрастающая последовательность элементов множества J. Однако если $i \in K$, то элемент x_i входит в ядро линейной формы $y \to F(x_j, y)$, то есть $i^F_{x_j}(x'_K) = 0$ (лемма 1). Это доказывает нужное утверждение.

Таким образом, мы доказали следующую теорему:

Теорема 1. *Пусть A-модуль E имеет базис $(x_i)_{i \in L}$ и множество индексов L наделено структурой совершенного порядка.*

Для любого конечного подмножества H множества L положим $x_H = \varrho(x_{h_1})\,\varrho(x_{h_2}) \ldots \varrho(x_{h_q})$, где $(h_1, \ldots, h_q)$ — строго возрастающая последовательность элементов множества H. Тогда элементы x_H образуют базис A-модуля $C(Q)$.

Следствие 1. *Если E — свободный модуль размерности n, то $C(Q)$ — свободный модуль размерности 2^n; кроме того, если $n > 0$, то C^+ и C^- — свободные модули размерности 2^{n-1}.*

Это сразу следует из свойств биномиальных коэффициентов.

Следствие 2. *Если E — свободный модуль, то каноническое отображение ϱ модуля E в $C(Q)$ и отображение $a \to a \cdot 1$ алгебры A в $C(Q)$ инъективны.*

Следствие 3. *Пусть E — прямая сумма двух свободных подмодулей E_1 и E_2, Q_i — сужение формы Q на E_i, и p_i — каноническое отображение алгебры $C(Q_i)$ в $C(Q)$ $(i = 1, 2)$. Тогда линейное отображение p тензорного произведения $C(Q_1) \otimes C(Q_2)$ в $C(Q)$, получаемое из билинейного отображения $(a, b) \to p_1(a)\, p_2(b)$ произведения $C(Q_1) \times C(Q_2)$ в $C(Q)$, является биекцией.*

В самом деле, достаточно рассмотреть базис модуля E, полученный объединением базисов модулей E_1 и E_2.

Следствие 4. *В обозначениях и предположениях следствия 3 предположим дополнительно, что подмодули E_1 и E_2 ортогональны, и перенесем с помощью биекции p структуру алгебры $C(Q)$ на тензорное произведение $C(Q_1) \otimes C(Q_2)$. Если a_i и b_i — четные или нечетные элементы алгебры $C(Q_i)$ $(i = 1, 2)$, то $(a_1 \otimes a_2)(b_1 \otimes b_2) = \varepsilon(a_1 b_1) \otimes (a_2 b_2)$, где $\varepsilon = 1$, за исключением случая, когда a_2 и b_1 нечетны, в котором $\varepsilon = -1$.*

В самом деле, достаточно доказать равенство $p_2(a_2)\, p_1(b_1) = \varepsilon p_1(b_1)\, p_2(a_2)$; при этом можно предположить, что $p_2(a_2)$ (соответственно $p_1(b_1)$) является произведением $x_1 \ldots x_h$ (соответственно $y_1 \ldots y_k$) элементов множества $\varrho_Q(E_2)$ (соответственно $\varrho_Q(E_1)$). Так как подмодули E_1 и E_2 ортогональны, то

$$x_i y_j + y_j x_i = \Phi(x_i, y_j) = 0,$$

откуда

$$x_1 \ldots x_h y_1 \ldots y_k = (-1)^{hk} y_1 \ldots y_k x_1 \ldots x_h.$$

Утверждения следствий 3 и 4 остаются верными, если не предполагать, что модули E_1 и E_2 свободны.

4. Структура алгебры Клиффорда

В этом n° предполагается, что A — *поле*, E — векторное пространство *конечной* размерности m над полем A и квадратичная форма Q *невырождена* (откуда по теореме 1 § 5, n° 1, следует, что m четно, если поле A имеет характеристику 2). Так как модуль E свободен, каноническое отображение ϱ инъективно (n° 3, след-

ствие 2 теоремы 1). Мы будем в дальнейшем отождествлять E с его образом в $C(Q)$.

Теорема 2. *Пусть размерность $m = 2r$ пространства E — четное число, а форма Q нейтральна* (§ 4, n° 2). *Тогда алгебра $C(Q)$ сепарабельна* (гл. VIII, § 7, n° 5, определение 1) *и изоморфна алгебре всех эндоморфизмов векторного пространства размерности 2^r над полем A. Если, кроме того, $m > 0$, то алгебра $C^+(Q)$ сепарабельна и является прямой композицией двух идеалов, изоморфных алгебре всех эндоморфизмов векторного пространства размерности 2^{r-1} над полем A.*

В самом деле, так как форма Q нейтральна, то пространство E можно разложить в прямую сумму вполне сингулярных подпространств N и P размерности r (§ 4, n° 2, следствие 2 теоремы 2). Сужение формы Q на N равно нулю, и поэтому подалгебра S алгебры $C(Q)$, порожденная подпространством N, отождествляется с внешней алгеброй этого подпространства (n° 3, лемма 4). Для любого элемента $n \in N$ обозначим через e'_n отображение $t \to nt$ алгебры S в себя.

Пусть $(n_1, \ldots, n_r)$ — некоторый базис подпространства N; обозначим через $(p_1, \ldots, p_r)$ базис подпространства P такой, что $\Phi(n_i, p_j) = \delta_{ij}$ (§ 4, n° 2, предложение 2). Пусть p' $(p \in P)$ — линейная форма $n \to \Phi(n, p)$ на N и i_p — эндоморфизм алгебры S, получающийся посредством факторизации из эндоморфизма $i_{p'}$ алгебры $T(N)$, определенного для формы p' утверждением леммы 1 n° 2. Тогда по формуле (5)

$$e'_n \circ i_p + i_p \circ e'_n = \Phi(n, p) \qquad (n \in N,\ p \in P). \tag{12}$$

Для $x = n + p \in E$ (где $n \in N$, $p \in P$) положим $s(x) = e'_n + i_p$. Ясно, что s будет линейным отображением пространства E в $\mathscr{L}(S)$. Из равенства

$$s(x)^2 = (e'_n + i_p)^2 = Q(n) + \Phi(n, p) = Q(x),$$

в силу формулы (12) и леммы 1 (n° 2), следует, что отображение s можно продолжить до гомоморфизма (также обозначаемого s) алгебры $C(Q)$ в $\mathscr{L}(S)$ (n° 1, предложение 1). Покажем, что этот гомоморфизм сюръективен. Отсюда, ввиду того что $C(Q)$ и $\mathscr{L}(S)$ имеют одинаковую размерность 2^{2r}, будет следовать, что s — изоморфизм, то есть первое наше утверждение верно.

В самом деле, пусть I — интервал $[1, r]$. Для любого подмножества H в I положим $H' = I - H$ и обозначим через n_H (соответственно p_H) произведение элементов n_i (соответственно p_i) для $i \in H$, расположенных в порядке возрастания индексов. Напомним, что элементы n_H образуют базис алгебры S (n° 3, теорема 1). Положим, наконец, $x_{H,K} = n_H p_I n_{K'}$ для любых двух подмножеств H и K множества I. Докажем, что элементы $s(x_{H,K})$ образа $s(C(Q))$ порождают $\mathscr{L}(S)$. Но если $j \overline{\in} H$, то по лемме 1 $s(p_j)(n_H) = i_{p_j}(n_H) = 0$, так как все n_i при $i \in H$ принадлежат ядру линейной формы $n \to \Phi(n, p)$ на подпространстве N; с другой стороны, по формуле (12) имеем

$$s(p_j)(n_j n_H) = (i_{p_j} \circ e'_{n_j})(n_H) = \Phi(p_j, n_j)\, n_H - n_j \cdot s(p_j)(n_H) = n_H.$$

Поскольку s — гомоморфизм, отсюда следует, что для любых двух подмножеств H и K множества I выполняются равенства $s(p_K)(n_H) = 0$, если $K \not\subset H$, и $s(p_K)(n_H) = \pm n_{H \pm K}$, если $K \subset H$. Но, по определению, при $M \subset I$ и $L \subset I$ $s(n_M)(n_L) = n_M n_L$, и произведение $n_M n_L$ равно нулю при $M \cap L \neq \varnothing$ и равно $\pm n_{M \cup L}$ в противоположном случае. Поэтому для любых подмножеств H, K, L множества I элемент $s(x_{H,K})(n_L) = s(n_H)\, s(p_I)\, s(n_{K'})(n_L)$ равен нулю при $K \neq L$ и равен $\pm n_H$ при $K = L$. Это означает, что элементы $s(x_{H,K})$ порождают алгебру $\mathscr{L}(S)$, так что первое утверждение доказано.

Для доказательства второго утверждения положим $S^+ = S \cap C^+$ и $S^- = S \cap C^-$; ясно, что S^+ (соответственно S^-) является подпространством в S, порожденным всеми элементами n_H, соответствующими множеству H с четным (соответственно нечетным) числом элементов, что S является прямой суммой подпространств S^+ и S^- и что S^+ и S^- устойчивы относительно $s(C^+)$. Следовательно, s отображает C^+ в некоторую подалгебру алгебры $\mathscr{L}(S)$, изоморфную произведению $\mathscr{L}(S^+) \times \mathscr{L}(S^-)$. Сужение отображения s на C^+ будет изоморфизмом C^+ на эту подалгебру, так как s инъективно, а C^+ и произведение $\mathscr{L}(S^+) \times \mathscr{L}(S^-)$ оба имеют размерность 2^{2r-1} (n° 2, следствие 1 теоремы 1). Теорема доказана.

Следствие. *Если m — четное число, но индекс формы Q произвольный, то алгебра $C(Q)$ является простой центральной алгеброй размерности 2^m. Если, кроме того, $m > 0$, то подалгебра*

$C^+(Q)$ сепарабельна и ее центр Z имеет размерность 2 над полем A. Если Z — поле, то оно является сепарабельным квадратичным расширением поля A и алгебра $C^+(Q)$ проста; в противоположном случае центр Z будет прямой композицией двух полей, изоморфных полю A, а алгебра $C^+(Q)$ будет прямой композицией двух простых алгебр размерности 2^{m-2}.

В самом деле, пусть A' — алгебраическое замыкание поля A, Q' — квадратичная форма на пространстве $E' = A' \otimes_A E$, полученная из формы Q расширением скаляров. Мы уже видели, что алгебра $C(Q')$ изоморфна $A' \otimes_A C(Q)$ (предложение 2). Ясно, что алгебра $C^+(Q')$ изоморфна $A' \otimes_A C^+(Q)$. Так как форма Q' нейтральна (§ 4, n° 2, следствие 2 предложения 1), то утверждение непосредственно следует из теоремы 2 и теорем перманентности гл. VIII, § 7.

Замечания. 1) Так как алгебра $C(Q)$ проста, она имеет единственный класс неприводимых представлений; эти представления называются *спинорными*; если выбрано одно из этих представлений, скажем τ, то элементы пространства, в котором действует τ, называются *спинорами*. Если форма Q нейтральна, то сужение представления τ на $C^+(Q)$, так же как и сужение формы s на $C^+(Q)$, будет суммой двух неэквивалентных абсолютно неприводимых представлений; элементы подпространств, в которых осуществляются эти два представления, называются *полуспинорами*. В общем случае, если алгебра $C^+(Q)$ не простая, сужение представления τ на $C^+(Q)$, будучи точным, должно содержать подпредставления, принадлежащие каждому из двух классов неприводимых представлений алгебры $C^+(Q)$, и, следовательно, будет суммой двух неэквивалентных абсолютно неприводимых представлений, поскольку это верно при расширении скаляров до алгебраического замыкания A' поля A. Напротив, если алгебра $C^+(Q)$ простая, она имеет единственный класс неприводимых представлений, и сужение представления τ на $C^+(Q)$ неприводимо, так как при расширении скаляров до поля A' τ распадается на два неэквивалентных представления.

2) Предположим, что характеристика поля A не равна 2, и пусть $(x_1, \ldots, x_m)$ $(m = 2r)$ — ортогональный базис пространства E.

Положим

$$z = 2^r x_1 \dots x_m \in C(Q).$$

Так как $x_i x_j + x_j x_i = 0$ для $i \neq j$, то $z x_j = -x_j z$, то есть элемент z входит в центр Z алгебры $C^+(Q)$ и не входит в A. Имеем

$$z^2 = 2^{2r}(-1)^r Q(x_1) \dots Q(x_m) = (-1)^r D,$$

где D — дискриминант формы Ф относительно базиса (x_j) (см. упражнение 9).

Теорема 3. *Пусть пространство E имеет нечетную размерность $m = 2r + 1$ (следовательно, характеристика поля A не равна 2).*

а) *Алгебра $C^+(Q)$ — центральная простая. Если форма Q имеет максимальный индекс r, то алгебра $C^+(Q)$ изоморфна алгебре всех эндоморфизмов векторного пространства размерности 2^r над полем A.*

б) *Алгебра $C(Q)$ сепарабельна. Ее центр Z имеет размерность 2, и $C(Q)$ изоморфна тензорному произведению $Z \otimes_A C^+(Q)$, то есть или проста, или является прямой композицией двух простых подалгебр.*

В самом деле, пусть x_0 — неизотропный вектор пространства E и F — подпространство, ортогональное к x_0; обозначим через Q_1 квадратичную форму $y \to -Q(x_0)Q(y)$ на пространстве E; ясно, что форма Q_1 невырождена. Так как $x_0 y = -y x_0$ (для $y \in F$), то $(x_0 y)^2 = -Q(x_0)Q(y) = Q_1(y)$, и следовательно, отображение $y \to x_0 y$ подпространства F в $C^+(Q)$ может быть продолжено до гомоморфизма h алгебры $C(Q_1)$ в $C^+(Q)$ (n° 1, предложение 1). Но алгебра $C(Q_1)$ проста (теорема 2), и ее размерность 2^{2r} — та же, что у алгебры $C^+(Q)$. Поэтому (ввиду того, что $h(1) = 1$) h — изоморфизм. Более того, если индекс формы Q равен r, то элемент x_0 можно выбрать таким образом, чтобы форма Q_1 также имела индекс r (§ 4, n° 2, предложение 3). Отсюда следует утверждение а).

Пусть теперь $(x_1, \dots, x_{2r})$ — ортогональный базис подпространства F; положим $z = x_0 x_1 \dots x_{2r}$. Непосредственно проверяется, что элемент z коммутирует с x_j при $j = 0, \dots, 2r$, то есть принадлежит центру алгебры $C(Q)$. Подпространство Z алгебры $C(Q)$, порожденное элементами I и z, является подалгеброй центра

алгебры $C(Q)$ и квадратичным расширением поля A, так как элемент z нечетный и z^2 равен скаляру $(-1)^r Q(x_0) \ldots Q(x_{2r})$.

Рассмотрим гомоморфизм ϑ тензорного произведения $Z \otimes_A C^+(Q)$ в $C(Q)$, определенный формулой $\vartheta(u \otimes v) = uv$. Так как элемент $z \in C^-$ обратим, отображение $u \to zu$ будет изоморфизмом модуля C^+ на C^-, откуда следует, что образ $\vartheta(Z \otimes C^+)$ содержит модули C^+ и C^-, то есть совпадает с алгеброй $C(Q)$. Так как алгебры $Z \otimes C^+$ и $C(Q)$ имеют одинаковую размерность 2^{2r+1}, ϑ — изоморфизм. Отсюда, в силу результатов гл. VIII, § 7, следует утверждение б).

Замечание. Дискриминант D формы Φ относительно базиса $(x_j)_{(j=0,\ldots,2r)}$ равен $2^{2r+1} Q(x_0) \ldots Q(x_{2r})$. Следовательно, подпространство Z порождается 1 и нечетным элементом $z' = 2^{r+1}z$ таким, что $z'^2 = (-1)^r 2D$. Следовательно, алгебра $C(Q)$ проста тогда и только тогда, когда элемент $2(-1)^r D$ не является квадратом в поле A.

5. *Группа Клиффорда*

В этом n° предполагается, что A — *поле*, пространство E имеет *конечную* размерность n и форма Q *невырождена*; при этом E отождествляется со своим каноническим образом в алгебре $C(Q)$.

Определение 2. *Группой Клиффорда формы* Q (соответственно *специальной группой Клиффорда формы* Q) *называется мультипликативная группа обратимых элементов* s *алгебры* $C(Q)$ (соответственно $C^+(Q)$) *таких, что* $sEs^{-1} = E$.

Группа Клиффорда и специальная группа Клиффорда формы Q обозначаются в этом n° G и G^+. Ясно, что $G^+ = G \cap C^+(Q)$.

Теорема 4. *Положим* $\varphi(s) \cdot x = sxs^{-1}$ *для* $s \in G$ *и* $x \in E$.

а) *Отображение* φ *является гомоморфизмом группы* G *в ортогональную группу* $\mathbf{O}(Q)$ *формы* Q, *и его ядро есть множество обратимых элементов центра* Z *алгебры* $C(Q)$.

б) *Множество* $E \cap G$ *представляет собой множество несингулярных векторов пространства* E; *при* $x \in E \cap G$ *отображение* — $\varphi(x)$ *является симметрией относительно гиперплоскости, ортогональной к вектору* x.

в) *Если* $\dim(E)$ *четна, то при* $E \neq \{0\}$ $\varphi(G) = \boldsymbol{O}(Q)$ *и* $\varphi(G^+)$ *имеет в* $\boldsymbol{O}(Q)$ *индекс* 2, *и* $\varphi(G^+)$ *совпадает с* $\boldsymbol{SO}(Q)$, *если поле* A *имеет характеристику* $\neq 2$.

г) *Если* $\dim(E)$ *нечетна* (*и, следовательно, характеристика поля* A *не равна* 2), *то* $\varphi(G) = \varphi(G^+) = \boldsymbol{SO}(Q)$.

В самом деле, для $s \in G$ и $x \in E$ имеем равенства $Q(sxs^{-1}) = (sxs^{-1})^2 = sx^2s^{-1} = Q(x)$, откуда $\varphi(s) \in \boldsymbol{O}(Q)$. Для выполнения равенства $\varphi(s) = 1$ необходимо и достаточно, чтобы элемент s коммутировал со всеми элементами из E, то есть принадлежал центру Z алгебры $C(Q)$. Это доказывает утверждение а).

Для того чтобы элемент $x \in E$ принадлежал группе G, необходимо, чтобы он был обратимым, то есть несингулярным (так как $x^2 = Q(x)$). Если же это так, то $x^{-1} = Q(x)^{-1}x$, откуда для любого $y \in E$ имеем

$$xyx^{-1} = Q(x)^{-1}xyx = Q(x)^{-1}x(\Phi(x, y) - xy) = -(y - \Phi(x, y)Q(x^{-1})x),$$

что и доказывает утверждение б) (§ 6, n° 4).

Лемма 5. *Всякий элемент* s *группы* G *имеет вид* zs', *где* z — *обратимый элемент центра* Z *и* s' *входит в* $G \cap C^+(Q)$ *либо в* $G \cap C^-(Q)$; *при* $E \neq 0$ *подгруппа* G^+ *имеет в группе* G *индекс* 2.

Второе утверждение, очевидно, следует из первого, так как все несингулярные векторы входят в пересечение $G \cap C^-(Q)$. Предположим сначала, что $\dim(E)$ четная, и пусть $s = t' + t''$, где $t' \in C^+(Q)$ и $t'' \in C^-(Q)$; по определению, для любого $s \in E$ имеем равенство $s(x) = (\varphi(s)\cdot x)\, t''$; так как элементы $t'x$ и $(\varphi(s)\cdot x)\, t'$ (соответственно $t''x$ и $(\varphi(s)\cdot x)\, t''$) нечетны (соответственно четны), то $t'x = (\varphi(s)\cdot x)\, t'$, и поэтому $s^{-1}t'x = xs^{-1}t'$ для любого $x \in E$. Отсюда следует, что $s^{-1}t' \in Z$, и, поскольку $\dim(E)$ четна, $Z = A$ (n° 4, следствие теоремы 2), то есть $t' = as$, где $a \in A$. Если $a \neq 0$, то $s = a^{-1}t'$ и $t' \in G \cap C^+(Q)$; если $a = 0$, то $s = t'' \in G \cap C^-(Q)$, и в рассматриваемом случае лемма доказана. Если $\dim(E)$ нечетна, так что характеристика поля A отлична от 2, то для любого $s \in G$ элемент $\varphi(s)$ является произведением симметрий относительно несингулярных векторов x_i $(i = 1, \ldots, h)$ (§ 6, n° 4, предложение 5); положив $s' = x_1x_2 \ldots x_h$, будем иметь $\varphi(s) = \varphi(s')$, то есть $s = zs'$, где $z \in S$, а s' входит в $C^+(Q)$ или в $C^-(Q)$, смотря по тому, четно h или нечетно.

Предположим, что размерность $\dim(E)$ четна. Так как всякий автоморфизм u из группы $\boldsymbol{O}(Q)$ однозначно продолжается до автоморфизма $\bar{u}$ алгебры $C(Q)$ (предложение 1) и $C(Q)$ — центральная простая алгебра (теорема 2), то $\bar{u}$ является внутренним автоморфизмом (гл. VIII, § 10, n° 1, теорема 1). Следовательно, в группе G существует элемент s такой, что $\varphi(s) = u$. С другой стороны, центр алгебры $C(Q)$ содержится в C^+, откуда следует, что факторгруппа $\varphi(G)/\varphi(G^+)$ изоморфна G/G^+, то есть если $E \neq \{0\}$, то $\varphi(G^+)$ имеет индекс 2 в группе $\varphi(G) = \boldsymbol{O}(Q)$. Это доказывает первые два утверждения в в).

Предположим, наконец, что поле A имеет характеристику $\neq 2$. Тогда всякий элемент u группы $\boldsymbol{O}(Q)$ является произведением симметрий относительно гиперплоскостей, ортогональных к несингулярным векторам x_i $(i = 1, \ldots, h)$ (§ 6, n° 4, предложение 5); следовательно, $u = (-1)^h \varphi(x_1 \ldots x_h)$ и $\det(u) = (-1)^h$. Для того чтобы автоморфизм u принадлежал группе $\boldsymbol{SO}(Q)$, необходимо и достаточно, чтобы h было четным; это показывает, что $\varphi(G^+) \supset \boldsymbol{SO}(Q)$. Если $E \neq \{0\}$ имеет *четную* размерность, то $\varphi(G^+) = \boldsymbol{SO}(Q)$, так как подгруппа $\boldsymbol{SO}(Q)$ в группе $\boldsymbol{O}(Q)$ имеет индекс 2, и утверждение в) доказано. Напротив, если размерность E *нечетна*, то $\varphi(G)$ не содержит ортогонального преобразования $x \to -x$. В самом деле, это преобразование продолжается до главного автоморфизма α алгебры $C(Q)$ (n° 1), и α не является внутренним автоморфизмом, так как центр Z алгебры $C(Q)$ содержит ненулевой элемент из $C^-(Q)$ (теорема 3). Следовательно, $\varphi(G) \neq \boldsymbol{O}(Q)$, и, поскольку $\varphi(G) \supset \Phi(G^+) \supset \boldsymbol{SO}(Q)$ и индекс подгруппы $\boldsymbol{SO}(Q)$ в $\boldsymbol{O}(Q)$ равен 2, имеем $\varphi(G) = \varphi(G^+) = \boldsymbol{SO}(Q)$, что и доказывает г).

Подгруппа $\varphi(G^+)$ группы $\boldsymbol{O}(Q)$, имеющая в случае $E \neq \{0\}$ индекс 2, называется *группой вращений* пространства E, а ее элементы — *вращениями*; обозначается эта группа $\boldsymbol{O}^+(Q)$. Заметим, что если поле A имеет характеристику, отличную от 2, то $\boldsymbol{O}^+(Q) = \boldsymbol{SO}(Q)$ (см. упражнение 9).

Предложение 4. *Пусть* β — *главный антиавтоморфизм алгебры* $C(Q)$ (n° 1). *Тогда для любого* $s \in G^+$ *элемент* $\beta(s)\,s$ *будет скаляром и отображение* $N\colon s \to \beta(s)\,s$ *является гомоморфизмом группы* G^+ *в мультипликативную группу* A^* *ненулевых элементов поля* A.

В самом деле, при $s \in G^+$ имеем $sEs^{-1} = E$, откуда $\beta(s)^{-1} E \beta(s) = E$, то есть $\beta(s) \in G^+$. Так как $sx = (\varphi(s) \cdot x)\, s$ для любого $x \in E$, то $x\beta(s) = \beta(sx) = \beta(s)(\varphi(s) \cdot x)$, и следовательно, $\beta(s)\, sx = \beta(s)(\varphi(s) \cdot x)\, s = x\beta(s)\, s$, так что $\beta(s)\, s$ входит в центр алгебры $C(Q)$. Поскольку, кроме того, $\beta(s)s \in C^+(Q)$, этот элемент является скаляром (теоремы 2 и 3). Наконец, $\beta(st)st = \beta(t)\beta(s)\, st = \beta(s)\, s\beta(t)\, t$, то есть $N(st) = N(s)\, N(t)$ для $s,\ t \in G^+$, что и требовалось доказать.

Скаляр $N(s) = \beta(s)s$ $(s \in G^+)$ называется *спинорной нормой* элемента s. Ядро гомоморфизма N называется *приведенной группой Клиффорда* и обозначается символом G_0^+. Образ $\varphi(G_0^+)$ обозначается $O_0^+(Q)$ и называется *приведенной ортогональной группой* формы Q.

Так как ядро сужения гомоморфизма φ на G^+ состоит из четных обратимых элементов центра алгебры $C(Q)$ (теорема 4) и, следовательно, отождествляется с A^* (теоремы 2 и 3), факторгруппа $\varphi(G^+)/O_0^+(Q)$ изоморфна $G^+/A^*G_0^+$, то есть изоморфна факторгруппе $N(G^+)/N(A^*)$, и, в частности, *коммутативна*. Ясно, что множество $N(A^*)$ является подгруппой $(A^*)^2$ квадратов элементов группы A^*. Если индекс формы Q больше 0, то для любого элемента $a \in A^*$ существуют два элемента x и $y \in E$ такие, что $Q(x) = a$ и $Q(y) = 1$ (§ 4, п° 2, предложение 4); так как $xy \in G^+$ и $N(xy) = Q(x)\, Q(y) = a$, отсюда следует равенство $N(G^+) = A^*$, так что факторгруппа $\varphi(G^+)/O_0^+(Q)$ изоморфна группе $A^*/(A^*)^2$.

Упражнения. *1) Доказать следствия 3 и 4 теоремы 1 п° 3 в случае, когда E_1 и E_2 — произвольные дополнительные подмодули в E. (Сначала доказать следствие 4; для этого показать, что тензорное произведение $C(Q_1) \otimes C(Q_2)$ после соглашения о выборе знака, сделанного в формулировке следствия 4, наделяется структурой алгебры и эта алгебра является решением той же проблемы универсального отображения, что и $C(Q)$; для этого вместе со всяким линейным отображением f модуля E в некоторую алгебру D над кольцом A таким, что $(f(x))^2 = Q(x) \cdot 1$, рассмотреть гомоморфизм $\bar{f}_i$ алгебры $C(Q_i)$ в D такой, что $\bar{f}_i = 1$, $\bar{f}_i(\varrho_{Q_i}(x_i)) = f(x_i)$ для $x_i \in E_i$ $(i = 1, 2)$, и доказать, что существует гомоморфизм $\bar{f}$ алгебры S в D такой, что

$$\bar{f}(z_1 \otimes z_2) = \bar{f}_1(z_1)\, \bar{f}_2(z_2)$$

для $z_i \in C(Q_i)$ $(i = 1, 2)$. Для доказательства следствия 3 рассмотреть внешнюю прямую сумму Q' форм Q_1 и Q_2 (§ 3, n° 4) и заметить, что $Q'(x) = Q(x) + F(x, x)$, где F — билинейная форма, определяемая равенством $F(x_1 + x_2, y_1 + y_2) = -\Phi(x_1, y_2)$ для $x_i, y_i \in E_i$ $(i = 1, 2)$; затем применить предложение 3.)

*2) Пусть модуль E является прямой суммой ортогональных подмодулей E_1, E_2, и Q_i — сужение формы Q на E_i $(i = 1, 2)$; предположим, что существует элемент $u \in C^+(Q_2)$ такой, что $u^2 = a \cdot 1$, где $a \in A$ — обратный элемент, и $u\varrho_{Q_2}(x_2) = -\varrho_{Q_2}(x_2)$ для любого $x_2 \in E_2$. Показать, что существует изоморфизм φ алгебры $C(Q)$ на тензорное произведение $C(aQ_1) \otimes C(Q_2)$ (определенный в гл. III, § 3, n° 1), обладающий свойством

$$\varphi(\varrho_Q(x)) = \varrho_{aQ_1}(x_1) \otimes u^{-1} + 1 \otimes \varrho_{Q_2}(x_2)$$

для любого $x = x_1 + x_2$ $(x_i \in E_i,\ i = 1, 2)$. (Существование гомоморфизма φ вывести как следствие универсального свойства алгебры $C(Q)$. С другой стороны, существует гомоморфизм g_1 алгебры $C(aQ_1)$ в $C(Q)$ такой, что $g_1(\varrho_{aQ_1}(x_1)) = h_2(u)\varrho_{Q_1}(x_1)$, где h_2 — канонический гомоморфизм алгебры $C(Q_2)$ в $C(Q)$; заметить, далее, что при $z_1 \in C(aQ_1)$ и $z_2 \in C(Q_2)$ элементы $g_1(z_1)$ и $h_2(z_2)$ перестановочны, откуда вывести существование гомоморфизма, обратного к φ.)

В каком случае этот результат применим, если A — поле характеристики $\neq 2$ (воспользоваться замечанием 2 после следствия к теореме 2)?

3) а) В обозначениях n° 2, пусть x_i $(1 \leqslant i \leqslant n)$ — элементы модуля E такие, что $f(x_i) = 0$; показать, что $i_f(x_1 \otimes x_2 \otimes \ldots \otimes x_n) = 0$. В частности, если билинейная форма F на модуле E удовлетворяет условию $F(x_i, x_j) = 0$ для $i > j$, то $i^F_{x_1}(x_2 \otimes x_3 \otimes \ldots \otimes x_n) = 0$.

б) В обозначениях предложения 3 n° 3, пусть x_i $(1 \leqslant i \leqslant n)$ — элементы модуля E такие, что $F(x_i, x_j) = 0$ при $i > j$. Показать, что $\overline{\lambda}_F(\varrho_{Q'}(x_1) \ldots \varrho_{Q'}(x_n)) = \varrho_Q(x_1) \ldots \varrho_Q(x_n)$ (использовать а) и формулу (10) n° 2).

в) Предположим, что A — поле характеристики $\neq 2$; для всякой квадратичной формы Q на модуле E обозначим через μ_Q отображение $\overline{\lambda}_F$ алгебры $C(Q)$ на $\bigwedge E$, соответствующее форме $F(x, y) = \frac{1}{2}\Phi(x, y)$. Показать, что если векторы x_i $(1 \leqslant i \leqslant n)$ попарно ортогональны, то

$$\mu_Q(x_1 x_2 \ldots x_n) = x_1 \wedge x_2 \wedge \ldots \wedge x_n.$$

Вывести отсюда, что для произвольных векторов y_i $(1 \leqslant i \leqslant n)$ справедливо равенство

$$n!\mu_Q^{-1}(y_1 \wedge y_2 \wedge \ldots \wedge y_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_\sigma y_{\sigma(1)} y_{\sigma(2)} \ldots y_{\sigma(n)}.$$

4) Пусть C_h — подмодуль алгебры $C(Q)$, порожденный произведениями k элементов из $\varrho_Q(E)$ для $0 \leqslant k \leqslant h$. Показать, что отображение

$$(x_1, \ldots, x_h) \to \varrho_Q(x_1) \ldots \varrho_Q(x_h)$$

путем факторизации определяет знакопеременное полилинейное отображение степени E^h в C_h/C_{h-1}. Получить из него линейное отображение π_h внешней степени $\bigwedge^h E$ в C_h/C_{h-1}; показать, что в случае, когда модуль E свободен, π_h является изоморфизмом. Для всякого ортогонального преобразования f имеет место равенство $C(f) \circ \pi_h = \pi_h \circ \bigwedge^h f$. Показать, что в случае, когда A — поле характеристики $\neq 2$, π_h является сужением отображения μ_Q^{-1}, определенного в упражнении 3в).

5) В обозначениях n° 2 рассмотрим отображение i_f модуля $\bigwedge E$ в себя. Доказать равенство

$$i_f(x_1 \wedge \ldots \wedge x_h) = \sum_{i=1}^{h} (-1)^{i-1} f(x_i)\, (x_1 \wedge \ldots \wedge x_{i-1} \wedge x_{i+1} \wedge \ldots \wedge x_h)$$

и вывести из него, что отображение i_f совпадает с правым внешним произведением $z \to z \llcorner f$ (гл. III, § 8, n° 4, определение 2).

6) Показать, что если модуль E имеет базис (e_1, e_2), ортогональный относительно формы Q, то алгебра $C(Q)$ изоморфна алгебре кватернионов над A, соответствующей паре (α_1, α_2), где $\alpha_i = Q(e_i)$ $(i = 1, 2)$.

7) Пусть A — максимальное упорядоченное поле, E — векторное пространство четной размерности $2r$ над полем A, Q — невырожденная квадратичная форма на пространстве, положительная или отрицательная. Показать, что если форма Q положительна, то при четном r $(r - 1)/2$ алгебра $C(Q)$ изоморфна некоторой алгебре матриц над A, а при нечетном r $(r - 1)/2$ $C(Q)$ изоморфна некоторой алгебре матриц над телом кватернионов над полем A. Если форма Q отрицательна, то $C(Q)$ изоморфна некоторой алгебре матриц над A при r $(r + 1)/2$ четном и изоморфна некоторой алгебре матриц над телом кватернионов над полем A при r $(r + 1)/2$ нечетном (использовать упражнения 2 и 6). Какова структура алгебры $C^+(Q)$ в этих двух различных случаях?

8) Пусть кольцо A есть $\boldsymbol{Z}/(4)$, E — A-модуль $\boldsymbol{Z}/(2)$; положив $Q(0) = 0$, $Q(u) = 1$ для единственного отличного от нуля элемента $u \in E$, получим квадратичную форму Q на пространстве E. Показать, что A-модули $C(Q)$ и $\bigwedge E$ не изоморфны (доказать, что модуль $C(Q)$ изоморфен прямой сумме модулей, изоморфных E).

*9) Пусть A — поле характеристики $\neq 2$, E — векторное пространство над A конечной четной размерности $2r$, Q — невырожденная квадратичная форма на пространстве E.

а) Пусть (e_i) — симплектический базис (§ 5, n° 1) пространства E относительно знакопеременной билинейной формы Ф, ассоциированной с Q. Показать, что элемент

$$z = e_1e_2 + e_3e_4 + \ldots + e_{2r-1}e_{2r}$$

алгебры $C^+(Q)$ образует вместе с единицей базис центра Z алгебры $C^+(Q)$. Для того чтобы центр Z был прямой суммой двух полей, необходимо и достаточно, чтобы элемент

$$\Delta(Q) = Q(e_1)\,Q(e_2) + Q(e_3)\,Q(e_4) + \ldots + Q(e_{2r-1})\,Q(e_{2r})$$

(называемый *псевдодискриминантом* формы Q относительно симплектического базиса (e_i)) имел вид $\lambda^2 + \lambda$, $\lambda \in A$.

б) Пусть u — подобие относительно Ф (§ 6, n° 5) с коэффициентом $\mu(u)$, и $Q_1(x) = Q(u(x))$. Положим

$$u(e_{2i-1}) = \sum_{j=1}^{r} a_{ij}e_{2j-1} + \sum_{j=1}^{r} b_{ij}e_{2j},$$

$$u(e_{2i}) = \sum_{j=1}^{r} c_{ij}e_{2j-1} + \sum_{j=1}^{r} d_{ij}e_{2j}$$

и $Q(e_{2i-1}) = \alpha_i$, $Q(e_{2i}) = \beta_i$ $(1 \leqslant i \leqslant r)$. Показать, что

$$\Delta(Q_1) = (\mu(u))^2\,\Delta(Q) + (D(u))^2 + \mu(u)\,D(u),$$

где

$$D(u) = \sum_{i,j} (\alpha_j a_{ij}c_{ij} + \beta_j b_{ij}d_{ij} + b_{ij}c_{ij})$$

(*инвариант Диксона* подобия u относительно базиса (e_i)). (Заметить, что элемент

$$(\mu(u))^{-1}(u(e_1)\,u(e_2) + u(e_3)\,u(e_4) + \ldots + u(e_{2r-1})\,u(e_{2r}))$$

принадлежит Z.) Для того чтобы u было подобием относительно Q (§ 4, упражнение 9) с коэффициентом $\mu(u)$, необходимо и достаточно, чтобы $D(u) = 0$ или $D(u) = \mu(u)$; подобия относительно Q такие, что $D(u) = 0$, называются *прямыми*.

в) Показать, что если v — подобие относительно Ф, u — подобие относительно Q, то

$$D(uv) = \mu(v)\,D(u) + \mu(u)\,D(v)$$

(рассмотреть инвариант Диксона подобия v относительно симплектического базиса, составленного из векторов $u(e_{2i-1})$ и $(\mu(u))^{-1}u(e_{2i})$ для $1 \leqslant i \leqslant r$). Вывести отсюда, что прямые подобия относительно Q образуют в группе подобий относительно Q нормальный делитель индекса 2.

г) Пусть u — симметрия относительно гиперплоскости, ортогональной к некоторому несингулярному вектору пространства E. Показать, что $D(u) = 1$. Вывести отсюда, что группа $\varphi(G^+)$

(обозначения из n° 5) совпадает с группой $\boldsymbol{SO}(Q)$, определенной в упражнении 28в) § 6.

д) Пусть поле A алгебраически замкнуто и $u \in \boldsymbol{O}(Q)$. Показать, что $u \in \boldsymbol{SO}(Q)$ тогда и только тогда, когда число элементарных делителей модуля E_u *четно*. (Заметить сначала, что, в обозначениях упражнения 15 § 5, число неразложимых подмодулей, в прямую сумму которых разлагается $G(p, q)$, где p, q — различные неприводимые множители минимального многочлена автоморфизма u, равно числу неразложимых подмодулей, на которые разлагается $G(q, p)$. Заметить, что, с другой стороны, $G(p, p) = \{0\}$ для всех p, кроме $p = X - 1$. Наконец, доказать, что можно ограничиться случаем, когда модуль E_u равен $G(p, p)$ $(p = X - 1)$ и неразложим. Тогда существует симплектический базис (e_i) пространства E такой, что векторы $e_1, e_3, \ldots, e_{2k-1}$ образуют базис в $(p(u))^{2r-k}(E)$, $1 \leqslant k \leqslant r$; показать, что векторы $e_1, e_3, \ldots, e_{2r-3}$ сингулярны, и получить, что $D(u) = 1$.)

*10) Пусть A — поле, E — конечномерное векторное пространство, Q — *вырожденная* квадратичная форма на E; пусть M — дополнение подпространства E^0 в E, B — (полупростая) алгебра Клиффорда сужения формы Q на M.

а) Предположим, что характеристика поля A не равна 2. Пусть L — алгебра Клиффорда сужения формы Q на E^0 (изоморфная $\bigwedge E^0$), $\mathfrak{R}_0$ — ее радикал (идеал, порожденный в L множеством E^0 факторразмерности 1 в L); показать, что радикал $\mathfrak{R}$ алгебры $C(Q)$ (с точностью до изоморфизма) получается при определении на $B \otimes \mathfrak{R}_0$ структуры алгебры, указанной в следствии 4 к теореме 1, что алгебра $C(Q)/\mathfrak{R}$ изоморфна B и что $C(Q)$ является прямой суммой алгебр B и $\mathfrak{R}$.

б) Предположим, что поле A имеет характеристику 2. Пусть F — подпространство в E^0, состоящее из *сингулярных* векторов $x \in E^0$, и N — дополнение F относительно E^0. Пусть $(a_i)_{1 \leqslant i \leqslant d}$ — базис N, $Q(a_i) = \alpha_i$, элементы $\alpha_i^{1/2}$ линейно независимы в алгебраическом замыкании поля A, и пусть $(\alpha_i^{1/2})_{1 \leqslant i \leqslant e}$ — 2-базис поля $A_1 = A(\alpha_1^{1/2}, \ldots, \alpha_d^{1/2})$ над A (гл. V, § 8, упражнение 1), $h = \dim F$, B_1 — центральная простая алгебра $B \otimes_A A_1$. Показать, что алгебра $C(Q)$ изоморфна алгебре $B_1 \otimes_{A_1} L_1$, где L_1 — внешняя алгебра векторного пространства размерности $h + d - e$ над A_1. Пусть $\mathfrak{R}_1$ — радикал алгебры L_1 (имеющий в L_1 коразмерность 1 над полем A_1). Показать, что радикал $\mathfrak{R}$ алгебры $C(Q)$ изоморфен алгебре $B_1 \otimes_{A_1} \mathfrak{R}_1$, что факторалгебра $C(Q)/\mathfrak{R}$ изоморфна B_1 и что $C(Q)$ есть прямая сумма алгебр B_1 и $\mathfrak{R}$.

в) В предположениях упражнения б) пусть $h = 0$, $d = 1$, $e = 0$ (откуда следует, что $\dim M$ четна). Показать, что алгебра $C^+(Q)$ изоморфна $C(Q_0)$, где Q_0 — сужение формы Q на M.

*11) а) В обозначениях и предположениях n° 5 показать, что группа $N(G^+)$ совпадает с подгруппой, порожденной в A^* произведениями $Q(x)\,Q(y)$, где x и y пробегают множество неизотропных векторов пространства E. (Свести доказательство к случаю $A \neq F_2$; использовать предложение 5 и упражнение 28в) § 6, а также упражнение 9г) § 9.) Это случай, когда индекс формы $Q \geqslant 1$.

б) Предположим, что $A \neq F_2$, и пусть размерность пространства E равна $n \geqslant 2$ и индекс формы Q положителен. Показать, что группа $O_0^+(Q)$ является коммутантом группы $O(Q)$. (Пользуясь упражнениями 17в) и 28д) § 6, свести доказательство к случаю $n = 2$.)

в) Сохраняя предположения б), будем считать дополнительно, что характеристика поля $\neq 2$ и размерность пространства E четна. Для того чтобы автоморфизм $x \to -x$ пространства E принадлежал группе $O_0^+(Q)$, необходимо и достаточно, чтобы дискриминант формы Q (относительно произвольного базиса пространства E) был квадратом.

*12) а) Пусть a — обратимый элемент кольца A; показать, что существует единственный изоморфизм ϑ_a алгебры $C^+(Q)$ на $C^+(aQ)$ такой, что

$$\vartheta_a(\varrho(x)\,\varrho(y)) = a^{-1}\varrho_1(x)\,\varrho_1(y)$$

для любых $x, y \in E$ (ϱ и ϱ_1 — канонические отображения пространства E в $C(Q)$ и $C(aQ)$ соответственно). Вывести отсюда, что если A — поле характеристики $\neq 2$, размерность векторного пространства E нечетна и форма Q невырождена, то алгебры $C(Q)$ и $C(aQ)$ изоморфны (см. упражнение 7).

б) Пусть A — поле, E — векторное пространство четной размерности $2r > 0$, Q — невырожденная квадратичная форма. Пусть u — подобие относительно Q; показать, что существует единственный A-автоморфизм $\bar{u}$ алгебры $C^+(Q)$ такой, что при $1 \leqslant h \leqslant r$ и $x_i \in E$ $(1 \leqslant i \leqslant 2h)$ выполняется равенство

$$\bar{u}(x_1x_2 \ldots x_{2h}) = \mu^{-h}u(x_1)\,u(x_2) \ldots u(x_{2h})$$

где μ — коэффициент подобия u. Автоморфизм $\bar{u}$ является внутренним тогда и только тогда, когда u — прямое подобие (§ 6, n° 5 и § 9, упражнение 9б)). Предположим еще, что $r \geqslant 2$; тогда, для того чтобы автоморфизм $\bar{u}$ был тождественным, необходимо и достаточно, чтобы u был гомотетией.

Показать, что автоморфизм $\bar{u}$ алгебры $C^+(Q)$ является сужением на $C^+(Q)$ некоторого внутреннего автоморфизма алгебры $C(Q)$.

*13) Пусть A — поле характеристики $\neq 2$, E — векторное пространство четной размерности $2r > 0$, Q — невырожденная квадратичная форма. Обозначим через E_h обратный образ степени $\bigwedge^h E$ при изоморфизме μ_Q из упражнения 3в), так что E_h является подпространством, порожденным в алгебре $C(Q)$ произведениями $x_1x_2 \ldots x_h$, где x_i $(1 \leqslant i \leqslant h)$ попарно ортогональны.

а) Пусть $\alpha \in A$, $s \in E_2$, $(\alpha + s)^2 \in A$. Показать, что либо $s = 0$, либо $a = 0$ и $s = xy$, где x и y — ортогональные векторы. (Выразив s через некоторый ортогональный базис пространства E, заметить, что элемент $t \wedge t$, где $t = \mu_Q(a + s)$, обязательно принадлежит $A + \overset{2}{\wedge} E$; используя § 5, n° 1, следствие 2 теоремы 1, вывести отсюда, что $t = \beta + x \wedge y$, где $\beta \in A$, $x, y \in E$.)

б) Пусть (x, y), (u, v) — две пары ортогональных неизотропных векторов пространства E, P_{xy} и P_{uv} — соответственно плоскости $Ax + Ay$ и $Au + Av$. Показать, что для выполнения равенства $(xy)(uv) = -(uv)(xy)$ в алгебре $C(Q)$ необходимо и достаточно, чтобы $P_{xy} + P_{uv}$ было неизотропным подпространством размерности 3, в котором P_{xy} и P_{uv} слабо ортогональны (§ 3, упражнение 11).

в) Пусть g — A-автоморфизм алгебры $C^+(Q)$, переводящий E_2 в себя; показать, что существует подобие u относительно Q такое, что $g = \bar{u}$ (упражнение 12б)). (Пусть $(e_i)_{1 \leqslant i \leqslant 2r}$ — некоторый ортогональный базис пространства E; пользуясь а) и б), показать, что найдется ортогональный базис (x_i) пространства E такой, что $g(e_1 e_i) = x_1 x_i$ для $2 \leqslant i \leqslant 2r$.)

14) Пусть A — поле характеристики $\neq 2$, E — векторное пространство размерности n над полем A, Q и Q_1 — невырожденные квадратичные формы на пространстве E; пусть $\tilde{\Delta}$ (соответственно $\tilde{\Delta}_1$) — класс дискриминанта Δ формы Q (соответственно дискриминанта Δ_1 формы Q_1) относительно некоторого базиса пространства E в группе $A^*/(A^*)^2$; этот класс не зависит от выбора базиса в E. Предположим, что $n = 2$.

а) Показать, что если $\tilde{\Delta} = \tilde{\Delta}_1$ и алгебры Клиффорда $C(Q)$ и $C(Q_1)$ изоморфны, то формы Q и Q_1 эквивалентны (рассмотреть на $C(Q)$ квадратичную форму $z \to z\bar{z}$, где $z \to \bar{z}$ — единственный инволютивный антиавтоморфизм алгебры $C(Q)$, у которого множеством инвариантных элементов является центр алгебры $C(Q)$ (см. упражнение 6 и гл. VIII, § 11, упражнение 5д)); применить теорему Витта).

б) Алгебра $C(Q)$ изоморфна алгебре матриц $M_2(A)$ тогда и только тогда, когда по крайней мере для одного вектора $x \neq 0$ пространства E найдутся такие y, $z \in E$, что $Q(x) + Q(y)\,Q(z) = 0$; в этом случае указанным свойством обладает всякий ненулевой вектор пространства E.

15) Сохраним обозначения и общие предположения упражнения 14, но положим $n = 3$.

а) Показать, что алгебра $C^+(Q)$ изоморфна некоторой алгебре кватернионов над A и что множество инвариантных элементов ее антиавтомофизма $\beta : z \to \bar{z}$ есть центр алгебры $C^+(Q)$. Пусть P — подпространство, составленное из *чистых* кватернионов алгебры $C^+(Q)$ (то есть таких, что $z = -\bar{z}$; гл. VIII, § 11, упражнение 6).

Сужение на P квадратичной формы $z \to z\bar{z}$ эквивалентно λQ, где $\lambda \in A$. Вывести отсюда, что $C^+(Q)$ является телом тогда и только тогда, когда форма Q имеет индекс 0.

б) Показать, что если $\widetilde{\Delta} = \widetilde{\Delta}_1$ и алгебры Клиффорда $C(Q)$ и $C(Q_1)$ изоморфны, то Q и Q_1 эквивалентны. (Рассмотреть сначала случай, когда $-\Delta$ является квадратом в A, и показать, что в этом случае алгебры $C^+(Q)$ и $C^+(Q_1)$ изоморфны; затем, применяя а) и упражнение 6 гл. VIII, § 11, рассуждать, как в упражнении 14а).)

в) Показать, что специальная группа Клиффорда G^+ (относительно формы Q) совпадает с группой обратимых элементов алгебры $C^+(Q)$. (Заметить, что отображение $x \to xj$, где $j = e_1e_2e_3 \in C(Q)$, (e_1, e_2, e_3) — ортогональный базис пространства E, является изоморфизмом пространства E на P.)

г) Вывести из а) и в), что если форма Q имеет индекс 1, то группа вращений $O^+(Q)$ изоморфна проективной группе $PGL_2(A)$ (гл. II, приложение III, n° 6).

*16) Сохраним обозначения и общие предположения упражнения 14, но положим $n = 4$.

а) Привести пример, в котором $\widetilde{\Delta} = \widetilde{\Delta}_1$, алгебры $C(Q)$ и $C(Q_1)$ изоморфны, но формы Q и Q_1 не эквивалентны (см. упражнение 7).

б) Пусть $(e_i)_{1 \leqslant i \leqslant 4}$ — ортогональный базис пространства E относительно Q, Q_0 — сужение формы Q на гиперплоскость $H = Ae_1 + Ae_2 + Ae_3$; показать, что алгебра $C^+(Q)$ изоморфна тензорному произведению $Z \otimes_A C^+(Q_0)$, где Z — ее центр. Для любого $z \in C^+(Q)$ имеем $\beta(z)\, z \in Z$; элемент z принадлежит специальной группе Клиффорда G^+ тогда и только тогда, когда z обратим и $\beta(z)\, z \in A \cdot 1$. Вывести отсюда, что группа $O_0^+(Q)$ изоморфна факторгруппе группы элементов $z \in Z \otimes_A C^+(Q_0)$ таких, что $\beta(z)\, z = 1$, по подгруппе $\{1, -1\}$.

в) Предположим, что Δ не является квадратом в поле A (откуда следует, ввиду теоремы Витта, что индекс формы Q равен 0 или 1). Пусть Q_0' — квадратичная форма, полученная из Q_0 расширением поля скаляров до $A' = A(\sqrt{\Delta})$; вывести из б), что группы $O_0^+(Q)$ и $O_0^+(Q_0')$ изоморфны. В частности, если индекс формы Q равен 1, то $O_0^+(Q)$ — коммутант группы $O(Q)$ и изоморфен группе $PSL_2(A')$ (см. упражнение 15г) и гл. III, § 7, упражнение 8).

г) Предположим, что Δ является квадратом в поле A (откуда следует, ввиду теоремы Витта, что индекс формы Q равен 0 или 2) и $Q(e_4) = 1$. Каждый элемент $x \in E$ единственным образом можно записать в виде $x = \alpha e_4 + jz$, где $j = e_1e_2e_3$, $\alpha \in A$, z — чистый кватернион (упражнение 15а)) из алгебры $L = C^+(Q_0)$; отображение ψ, где $\psi(x) = \alpha + z$, является изоморфизмом векторного пространства E на L. Пусть $Z = Ac' + Ac''$, где c' и c'' — ортогональные идемпотенты из центра Z; всякий обратимый элемент $s \in C^+(Q)$ един-

ственным образом может быть записан в виде $s = uc' + vc''$, где u и v принадлежат L; элемент s принадлежит специальной группе Клиффорда G^+ тогда и только тогда, когда $u\overline{u} = v\overline{v}$, и в этом случае $\psi(sxs^{-1}) = u\psi(x)v^{-1}$ для любого $x \in E$. Вывести отсюда, что факторгруппа группы $\boldsymbol{O}_0^+(Q)$ по ее центру (состоящему из двух элементов. см. упражнение 11в)) изоморфна произведению $\boldsymbol{O}_0^+(Q_0) \times \boldsymbol{O}_0^+(Q_0)$; в частности, если форма Q индекса 2, то эта факторгруппа изоморфна $\boldsymbol{PSL}_2(A) \times \boldsymbol{PSL}_2(A)$.

17) Пусть K — поле характеристики $\neq 2$, A — поле $K(X_n)_{n\in\boldsymbol{N}}$ рациональных дробей над полем K от счетного множества переменных (гл. IV, § 3, n° 1). Пусть E — векторное пространство над полем A со счетным базисом $(e_n)_{n\in\boldsymbol{N}}$, Φ — симметрическая билинейная форма на пространстве E, относительно которой базис (e_n) ортогонален, и $\Phi(e_n, e_n) = X_n$ для всех $n \in \boldsymbol{N}$. Положив $Q(x) = \Phi(x, x)$, показать. что алгебра Клиффорда $C(Q)$ —тело (см. гл. VIII, § 12, упражнение 14).

§ 10. Углы

В этом параграфе приняты обозначения: A — поле характеристики $\neq 2$, E — векторное пространство размерности 2 над полем A, Φ — невырожденная симметрическая билинейная форма на пространстве E.

1. Прямые подобия в плоскости

Напомним (§ 6, n° 5), что прямым подобием векторного пространства E называется такой его автоморфизм u, что $\Phi(u(x), u(y)) = (\det u)\Phi(x, y)$ для любых $x, y \in E$.

Предложение 1. *Пусть $A(\Phi)$ — подалгебра алгебры $\mathscr{L}_A(E)$, порожденная прямыми подобиями пространства E.*

а) *Прямые подобия являются обратимыми элементами подалгебры $A(\Phi)$. Алгебра $A(\Phi)$ коммутативна и имеет степень 2 над полем A. Если в пространстве E нет ненулевых неизотропных векторов, то $A(\Phi)$ — поле, являющееся квадратичным расширением поля A; в противоположном случае алгебра $A(\Phi)$ будет прямой композицией двух полей, изоморфных полю A.*

б) *Пусть (e_1, e_2) — ортогональный базис плоскости E. Положим $\alpha_i = \Phi(e_i, e_i)$ $(i = 1, 2)$ и $\delta = -\alpha_2/\alpha_1$. Тогда матрица любого элемента алгебры $A(\Phi)$ относительно этого базиса имеет вид $\begin{pmatrix} a & \delta b \\ b & a \end{pmatrix}$, где $a \in A$, $b \in A$.*

в) *Плоскость E является моногенным свободным A (Ф)-модулем и порождается любым неизотропным вектором.*

В самом деле, введем на плоскости E вспомогательную знакопеременную билинейную форму $B \neq 0$; форма B невырождена. Следовательно, существует эндоморфизм w плоскости E такой, что $\Phi(x, y) = B(w(x), y)$ для любых $x, y \in E$. Тогда для любого обратимого эндоморфизма u плоскости E имеем

$$\Phi(u(x), u(y)) = B(wu(x), u(y)) = B(uu^{-1}wu(x), u(y)) = \\ = (\det u)\, B(u^{-1}wu(x), y).$$

Следовательно, для того чтобы эндоморфизм u был прямым подобием, необходимо и достаточно, чтобы для любых $x, y \in E$ выполнялось равенство

$$(\det u)\, B(u^{-1}wu(x), y) = (\det u)\, \Phi(x, y) = (\det u)\, B(w(x), y).$$

Но $\det u \neq 0$, а форма B невырождена, то есть это равенство равносильно $u^{-1}wu = w$ или $uw = wu$. Выберем в качестве формы B знакопеременную форму, имеющую относительно базиса (e_1, e_2) матрицу $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$; обозначив через R и W матрицы формы Φ и эндоморфизма w относительно этого базиса и пользуясь формулой (47) § 1, n° 10, перепишем равенство $\Phi(x, y) = B(w(x), y)$ в виде $R = {}^tW \cdot S$; в явном виде это означает, что $W = \begin{pmatrix} 0 & \alpha_2 \\ -\alpha_1 & 0 \end{pmatrix}$. Если матрицу эндоморфизма u относительно базиса (e_1, e_2) обозначить через $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$, то равенство $uw = wu$ будет равносильно системе соотношений $b\alpha_2 = -c\alpha_1$, $a\alpha_2 = d\alpha_2$, $a\alpha_1 = d\alpha_1$, то есть $a = d$, $c = \delta b$; таким образом, матрицы прямых подобий являются обратимыми матрицами вида $\begin{pmatrix} a & \delta b \\ b & a \end{pmatrix}$ $(a, b \in A)$.

Но эндоморфизмы плоскости E, имеющие матрицы вида $\begin{pmatrix} a & \delta b \\ b & a \end{pmatrix}$ $(a, b \in A)$, образуют в $\mathscr{L}_A(E)$ векторное подпространство размерности 2, порожденное эндоморфизмами 1 и w; так как эндоморфизм w^2 является гомотетией, соответствующей элементу $-\alpha_1\alpha_2$, полученное подпространство составляет в $\mathscr{L}_A(E)$ подалгебру A (Ф), порожденную прямыми подобиями. Прямые подобия являются обратимыми элементами подалгебры A (Ф), то есть

элементами, матрицы которых удовлетворяют условию $a^2 - \delta b^2 = 0$. Очевидно, алгебра A (Ф) коммутативна. Применим к этой алгебре результаты гл. II, § 7, n° 7: если элемент δ не является квадратом в поле A, то есть все отличные от нуля векторы плоскости E неизотропны, то A (Ф) будет полем; если же, напротив, δ является квадратом в поле A, то есть плоскость E содержит ненулевые изотропные векторы, то A (Ф) будет прямой композицией двух полей, изоморфных A. Это доказывает утверждения а) и б).

Наконец, всякий неизотропный вектор плоскости E можно взять в качестве первого вектора e_1 ортогонального базиса (e_1, e_2) (§ 6, n° 1); следовательно, его образами $u(e_1)$ для всякого $u \in A$ (Ф) будут векторы вида $ae_1 + be_2$, а поскольку всякая матрица вида $\begin{pmatrix} a & \delta b \\ b & a \end{pmatrix}$ является матрицей некоторого элемента $u \in A$ (Ф), то среди образов $u(e_1)$ вектора e_1 будут все векторы плоскости E. Иными словами, плоскость E является моногенным A(Ф)-модулем, порожденным любым неизотропным вектором.

Более того, моногенный A(Ф)-модуль E свободен: если $u(e_1) = ae_1 + be_2 = 0$, то $a = b = 0$, то есть $u = 0$. Утверждение в) доказано.

Замечания. 1) Пусть v — подобие, имеющее относительно базиса (e_1, e_2) матрицу $\begin{pmatrix} 0 & \delta \\ 1 & 0 \end{pmatrix}$; подобие w, рассмотренное в доказательстве предложения 1, равно $-\alpha_1 v$; коэффициент прямого подобия $u = a + bv$ $(a, b \in A)$ равен определителю его матрицы $\begin{pmatrix} a & \delta b \\ b & a \end{pmatrix}$, то есть, в силу равенства $v^2 = \delta$, $a^2 - \delta b^2 = (a + bv)(a - bv) = u\bar{u}$, где $\bar{u}$ — элемент алгебры A (Ф), сопряженный подобию u (гл. II, § 7, n° 7); другими словами, коэффициент прямого подобия u равен его *норме* $N(u)$ в алгебре A (Ф) (там же). В частности, прямое подобие u тогда и только тогда будет вращением, когда $N(u) = 1$, и гомотетией, когда $u \in A^*$.

2) Из равенства $(a + bv)^2 = a^2 + \delta b^2 + 2abv$ следует, что прямые подобия $u = a + bv$ $(a, b \in A, b \neq 0)$, *квадрат* которых является гомотетией, сами являются гомотетиями bv, кратными подобию v. Такое прямое подобие представляет собой автоморфизм векторного пространства E, *переводящий каждый вектор в ему ортогональный*. В самом деле, матрица такого автоморфизма

должна иметь вид $\begin{pmatrix} a & c \\ d & 0 \end{pmatrix}$ $(c, d \in A)$, а условие, что вектор $\lambda e_1 + \mu e_2$ ортогонален к своему трансформированному вектору, можно записать в виде $\lambda\mu(d\alpha_2 + c\alpha_1) = 0$.

3) Легко видеть, что для любых $x, y \in E$ и $u \in A$ (Ф) справедливо равенство $\Phi(u(x), y) = \Phi(x, \bar{u}(y))$. Таким образом, эндоморфизм, *сопряженный* прямому подобию $\bar{u}$ (§ 1, n° 8), является прямым подобием $\bar{u}$, *сопряженным с* u в алгебре A (Ф) (гл. II, § 7, n° 7).

4) Так как всякое *обратное подобие* пространства E есть произведение некоторого прямого подобия и симметрии относительно подпространства Ae_1, то матрица обратного подобия относительно базиса (e_1, e_2) имеет вид $\begin{pmatrix} a & -\delta b \\ b & -a \end{pmatrix}$.

Далее мы будем применять обозначения: S — группа подобий плоскости E, S^+ — группа прямых подобий, H — группа ненулевых гомотетий, O^+ — группа вращений плоскости E. Напомним, что $H \subset S^+$ (§ 6, n° 5).

Следствие 1. *Группа S^+ прямых подобий коммутативна. Для любых неизотропных векторов x, y плоскости E существует единственное прямое подобие u такое, что $y = u(x)$.*

Первое утверждение следует из коммутативности алгебры A (Ф). Но E — моногенный свободный A (Ф)-модуль, порожденный элементом x (соответственно y), так что существует единственный элемент $u \in A$ (Ф) (соответственно $u' \in A$ (Ф)) такой, что $y = u(x)$ (соответственно $x = u'(y)$); отсюда $x = u(u'(x))$, то есть произведение uu' — тождественное отображение; это означает, что отображение u обратимо, то есть является прямым подобием.

Следствие 2. *Группа вращений O^+ коммутативна. Для любых векторов x, y плоскости E, удовлетворяющих условию $\Phi(x, x) = \Phi(y, y) \neq 0$, существует единственное вращение u такое, что $y = u(x)$.*

Первое утверждение верно в силу следствия 1. По этому же следствию существует единственное прямое подобие u такое, что $y = u(x)$; но $\Phi(u(x), u(x)) = \Phi(x, x)$, так что коэффициент подобия u равен 1, то есть u — вращение.

Следствие 3. *Группа S^+/H коммутативна. Она действует на множестве неизотропных прямых плоскости E. Для любых неизо-*

тропных прямых D и D' плоскости E существует единственный элемент φ группы S^+/H такой, что $D' = \varphi(D)$.

Эти утверждения вытекают из следствия 1 и из того, что всякая прямая в плоскости E инвариантна относительно группы H.

Предложение 2. *Ядром канонического гомоморфизма группы O^+ в S^+/H является группа $\{1, -1\}$.*

В самом деле, 1 и -1 являются единственными элементами пересечения $H \cap O^+$.

Предложение 3. *Гомоморфизм $u \to u/\bar{u} = u^2/N(u)$ группы S^+ в себя имеет ядро H и посредством факторизации определяет изоморфизм факторгруппы S^+/H на O^+.*

В самом деле, равенство $u/\bar{u} = 1$ равносильно $u = \bar{u}$, то есть $u \in A^* = H$; следовательно, подгруппа H является ядром отображения $u \to u/\bar{u}$. Так как $N(u/\bar{u}) = 1$, то $u/\bar{u}$ — вращение (замечание 1). Остается доказать, что всякий элемент $v \in O^+$ имеет вид $u/\bar{u}$ ($u \in S^+$). Если элемент $1 + v$ обратим, то в качестве u можно взять элемент $1 + \bar{v}$: $1 + v = v(1 + \bar{v})$, так как $N(v) = v\bar{v} = 1$. Если же это неверно, то $N(1 + v) = (1 + v) \times (1 + \bar{v}) = 0$, то есть, положив $v = a + bw$ ($a \in A$, $b \in A$, $w^2 = \delta \in A$), будем иметь равенство $2(1 + a) = 0$, откуда $a = -1$; но тогда из равенств $a = -1$ и $N(v) = a^2 - \delta b^2 = 1$ следует, что $b = 0$, то есть $v = -1$; а в этом случае, так как $\bar{w} = -w$, можно взять $u = w$.

Если A (Ф) — поле, то предложение 3 является частным случаем теоремы Гильберта (гл. IV, § 11, п° 5, теорема 3).

Следствие. *Пусть i: $O^+ \to S^+/H$ и d: $S^+/H \to O^+$ — гомоморфизмы, построенные в предложениях 2 и 3; если композиции в абелевых группах O^+ и S^+/H записываются аддитивно, то $d(i(\theta)) = 2\theta$ для $\theta \in O^+$ и $i(d(\varphi)) = 2\varphi$ для $\varphi \in S^+/H$.*

В самом деле, для любого вращения $\bar{v}$ имеем $\bar{v} = v^{-1}$, откуда $d(i(v)) = v/\bar{v} = v^2$. С другой стороны, если $\varphi \in S^+/H$, то φ является классом по mod H некоторого подобия u, и элемент $d(\varphi) = u/\bar{u} = u^2/N(u)$ попадает в тот же смежный класс mod H, что и элемент u^2; отсюда следует вторая формула.

2. *Плоская тригонометрия*

В этом n° мы выберем некоторый образующий элемент w алгебры A (Ф), удовлетворяющий условию $w^2 \in A$. Такой образующий определяется с точностью до некоторой гомотетии (n° 1, замечание 2), так что элемент $w^2 \in A$, обозначенный ниже через δ, определен по модулю мультипликативной группы $(A^*)^2$ *квадратов* ненулевых элементов поля A.

Замечание. В случае, когда класс по mod $(A^*)^2$, о котором идет речь, содержит -1, элемент w обычно выбирают таким образом, чтобы $w^2 = -1$; это соотношение определяет w с точностью до знака. Если же этот класс не содержит -1, но содержит 1, то элемент w обычно выбирают таким образом, чтобы $w^2 = 1$, что также определяет w с точностью до знака.

Выбрав элемент w, мы можем всякий элемент $v \in S^+$ записать, и притом единственным способом, в виде

$$v = c_w(v) + s_w(v)\, w, \tag{1}$$

где $c_w(v)$, $s_w(v)$ — элементы поля A; элемент $s_w(v)/c_w(v)$ проективного поля $\widetilde{A}$ (гл. II, приложение III, n° 5) обозначается $t_w(v)$; этот элемент не зависит от класса элемента v по mod H и определяет, следовательно, посредством факторизации отображение факторгруппы S^+/H в проективное поле $\widetilde{A}$, которое мы, допуская вольность речи, также будем обозначать через t_w. Часто мы будем писать s, c и t вместо s_w, c_w и t_w. Очевидно, $c_{-w} = c_w$, $s_{-w} = -s_w$ и $t_{-w} = -t_w$.

Предложение 4. а) *Если элемент $w^2 = \delta$ не является квадратом в поле A (то есть плоскость E не имеет изотропных прямых), то отображение t факторгруппы S^+/H в $\widetilde{A}$ биективно.*

б) *Если элемент δ является квадратом некоторого элемента $\gamma \in A$, то отображение t будет биекцией группы S^+/H на поле $\widetilde{A}$, из которого исключены элементы $1/\gamma$ и $-1/\gamma$.*

в) *Записывая группу S^+/H аддитивно, для любых $\varphi, \varphi' \in S^+/H$ будем иметь*

$$t(\varphi + \varphi') = (t(\varphi) + t(\varphi'))/(1 + \delta t(\varphi))\, t(\varphi'), \tag{2}$$

если $t(\varphi)$ и $t(\varphi')$ конечны и $1 + t(\varphi)\, t(\varphi') \neq 0$.

В самом деле, группа S^+/H является множеством прямых (с исключительной точкой O) алгебры A/Φ, рассматриваемой как векторная плоскость над полем A, так что отображение t инъективно. С другой стороны, для того чтобы элемент $a + bw$ ($a \in A$, $b \in A$) алгебры A (Φ) был прямым подобием, необходимо и достаточно, чтобы он был обратимым, то есть чтобы выполнялось условие $N(a + bw) = a^2 - \delta b^2 \neq 0$, так что еще должно быть $(b/a)^2 \neq \delta$; отсюда следует сюръективность в утверждениях а) и б). Наконец, произведение подобий $1 + t(\varphi)\, w$ и $1 + t(\varphi')\, w$ есть подобие $1 + \delta t(\varphi)\, t(\varphi') + (t(\varphi) + t(\varphi'))\, w$, что доказывает утверждение в).

Предложение 5. *Будем записывать группу O^+ аддитивно. Для любой пары элементов $\theta, \theta' \in O^+$ имеем*

$$c(\theta)^2 - \delta s(\theta)^2 = 1, \tag{3}$$

$$c(\theta + \theta') = c(\theta)\, c(\theta') + \delta s(\theta)\, s(\theta'), \tag{4}$$

$$s(\theta + \theta') = s(\theta)\, c(\theta') + c(\theta)\, s(\theta'). \tag{5}$$

В самом деле, равенство (3) показывает, что $N(c(\theta) + s(\theta)\, w) = 1$. Для доказательства равенств (4) и (5) достаточно вычислить в алгебре A (Φ) произведение вращений $c(\theta) + s(\theta)\, w$ и $c(\theta') + s(\theta')\, w$.

Предложение 6. *Пусть d — изоморфизм группы S^+/H на O^+, определенный в предложении 3. Для любого элемента $\varphi \in S^+/H$ такого, что $t = t(\varphi)$ конечно, выполняются равенства*

$$s(d(\varphi)) = 2t/(1 - \delta t^2), \quad c(d(\varphi)) = (1 + \delta t^2)/(1 - \delta t^2). \tag{6}$$

В самом деле, элемент φ есть класс по mod H подобия $1 + tw$ и вращение $d(\varphi)$ равно, следовательно, $(1 + tw)^2/N(1 + tw) = (1 + \delta t^2 + 2tw)/(1 - \delta t^2)$ (предложение 3), что и доказывает (6).

Следствие. *Для любого элемента $\theta \in O^+$ такого, что $t(\theta)$ конечно, выполняются равенства*

$$s(2\theta) = 2\,\mathrm{tg}(\theta)/(1 - \delta t(\theta)^2), \quad c(2\theta) = (1 + \delta t(\theta)^2)/(1 - \delta t(\theta)^2). \tag{7}$$

Для любого элемента $\varphi \in S^+/H$ такого, что $t(\varphi)$ конечно

и $1 + \delta t(\varphi)^2 \neq 0$, *выполняется равенство*

$$t(2\varphi) = 2t(\varphi)/(1 + \delta t(\varphi)^2). \qquad (8)$$

В самом деле, это легко следует из предложения 6 и следствия к предложению 3.

Замечание. Формулы (6) останутся справедливыми и при $t = \infty$, если заменить рациональные функции, стоящие в правых частях, их каноническими продолжениями на проективное поле $\tilde{A}$ (гл. II, приложение III, n° 5); в самом деле, если $t = \infty$, то φ есть класс элемента w и выполняются равенства $d(\varphi) = -1$, $s(d(\varphi)) = 0$, $c(d(\varphi)) = -1$. Эти же значения принимают при $t = \infty$ канонические продолжения правых частей равенств (6). То же самое верно и для равенств (7), если $t(\vartheta) = \infty$, и для равенства (8), если $t(\varphi) = \infty$ или $1 + \delta t(\varphi)^2 = 0$. Точно так же формула (2) остается в силе, когда один из элементов $t(\varphi)$ и $t(\varphi')$, например $t(\varphi)$, бесконечен, если правую часть рассматривать как рациональную функцию только от $t(\varphi)$: в самом деле, произведение подобий $1 + t(\varphi')w$ и w равно $\delta t(\varphi') + w$, в то время как каноническое продолжение правой части равенства (2) принимает значение $1/\delta t(\varphi')$. Наконец, если $t(\varphi)$ и $t(\varphi')$ конечны и $1 + \delta t(\varphi)\, t(\varphi') = 0$, то $t(\varphi) + t(\varphi') \neq 0$ (иначе $t(\varphi)^2$ равнялось бы $1/\delta$, что невозможно (предложение 4)); следовательно, можно условиться, что значение правой части равенства (2) в этом случае равно ∞, и тогда оно совпадает со значением левой части. Если отношения $t(\varphi)$ и $t(\varphi')$ оба бесконечны, то правая часть равенства (2) не определена.

3. *Углы*

В этом и следующем n° мы предполагаем, что A — упорядоченное поле и, следовательно, его характеристика равна нулю. Напомним (Исправления к гл. VI), что отношение «существует $\lambda > 0$ такое, что $y = \lambda x$», определенное на векторном пространстве F над полем A, является отношением эквивалентности между элементами $x, y \in F - \{0\}$, что классы эквивалентности для этого отношения называются *открытыми полупрямыми* с началом 0 и что объединение открытой полупрямой и $\{0\}$ называется *замкнутой полупрямой* (или просто *полупрямой*) с началом 0. Если замкнутая полупрямая Δ содержится в прямой D, то D является объединением полупрямых Δ и $-\Delta$ и не содержит других замкнутых полупрямых. Мы будем называть полупрямую изотропной, если изотропна содержащая ее прямая.

Напомним еще (там же), что *ориентация* векторного пространства F *конечной* размерности n над полем — это задание

одной из двух полупрямых из пространства $\bigwedge^n F$; векторы, принадлежащие этой полупрямой, называются *положительными*. Векторное пространство конечной размерности, наделенное ориентацией, называется *ориентированным*.

Гомотетии плоскости E, соответствующие строго положительным элементам поля A, образуют, очевидно, в группе H подгруппу индекса 2; обозначим ее H^+. Канонический гомоморфизм $i: O^+ \to S^+/H$ (см. предложение 2) является композицией канонических гомоморфизмов группы S^+/H^+ на S^+/H и группы O^+ в S^+/H^+. Так как $O^+ \cap H^+ = \{1\}$, то последний гомоморфизм *инъективен*.

Предложение 7. *Пусть A — максимальное упорядоченное поле и* Ф — *положительная форма* (§ 7). *Тогда канонические гомоморфизмы группы O^+ в S^+/H^+ и группы $O^+/\{1, -1\}$ в S^+/H биективны и группа S^+ изоморфна группе $O^+ \times H^+$.*

Мы уже видели, что эти гомоморфизмы инъективны, и поэтому достаточно доказать, что первый из них сюръективен. Пусть (e_1, e_2) — ортонормальный базис плоскости E, а w — прямое подобие такое, что $w(e_1) = e_2$ (следствие 1 предложения 1, n° 1); тогда $w^2 = -1$ (предложение 1б)). Если $u = a + bw$ ($a \in A$, $b \in A$) — произвольное прямое подобие, то $N(u) = a^2 + b^2 > 0$ и существует единственное вращение, содержащееся в той же полупрямой плоскости A (Ф), что и подобие u, именно $(a^2 + b^2)^{1/2}$, что и доказывает наше утверждение.

Следствие. *Для любых двух полупрямых D и D' с началом 0 существует единственное вращение v такое, что $v(D) = D'$.*

В самом деле, из наших предположений следует, что в плоскости E нет изотропных прямых, и утверждение следствия сразу получается из следствия 1 к предложению 1 (n° 1).

Теперь мы будем предполагать, что A — *максимальное упорядоченное поле* и что форма Ф *положительна*. Определенное на множестве пар (D_1, D_2) прямых (соответственно полупрямых с началом 0) в плоскости E отношение «существует прямое подобие (соответственно вращение) u такое, что $u(D_1) = D_1'$ и $u(D_2) = D_2'$» является отношением эквивалентности между парами (D_1, D_2) и (D_1', D_2'). Класс эквивалентности, содержащий пару (D_1, D_2),

называется, по определению, *углом между прямыми* (соответственно между *полупрямыми*) D_1 и D_2 (взятыми в данном порядке); этот угол обозначается $\widehat{(D_1, D_2)}$.

Предложение 8. *Пусть A — максимальное упорядоченное поле и форма Φ положительна. Пусть, далее, D_1, D_2, D_1', D_2' — четыре прямые* (соответственно *полупрямые с началом* 0) *в плоскости E. Для того чтобы углы $\widehat{(D_1, D_2)}$ и $\widehat{(D_1', D_2')}$ были равны, необходимо и достаточно, чтобы были равны углы $\widehat{(D_1, D_1')}$ и $\widehat{(D_2, D_2')}$.*

Докажем необходимость этого условия. Пусть u — прямое подобие (соответственно вращение) такое, что $u(D_1) = D_1'$ и $u(D_2) = D_2'$. По следствию 3 предложения 1 (соответственно по следствию предложения 7) существует прямое подобие (соответственно вращение) v такое, что $v(D_1) = D_2$. Так как группа S^+ (соответственно O^+) *коммутативна*, то $D_2' = u(v(D_1)) = v(u(D_1)) = v(D_1')$, то есть $\widehat{(D_1, D_1')} = \widehat{(D_2, D_2')}$. Поменяв местами D_2 и D_1', из необходимости этого условия можно вывести достаточность.

Из предложения 8 следует, что с каждым углом $\widehat{(D_1, D_2)}$ между прямыми (соответственно полупрямыми с началом 0) в плоскости канонически ассоциируется однозначно определяющийся элемент группы S^+/H (соответственно O^+), именно класс по mod H прямых подобий v (соответственно вращение v) таких, что $u(D_1) = D_2$ для любого представителя (D_1, D_2) угла $\widehat{(D_1, D_2)}$. Тем самым определена *каноническая биекция* h (соответственно h') множества $\mathfrak{A}_0$ углов между прямыми (соответственно множества $\mathfrak{A}$ углов между полупрямыми) на группу S^+/H (соответственно O^+); в частности, элемент $h(\varphi)$ для любого $\varphi \in \mathfrak{A}$ называется *вращением на угол* φ. С помощью биекций h^{-1} и h'^{-1} перенесем на множества $\mathfrak{A}_0$ и $\mathfrak{A}$ структуры коммутативных групп S^+/H и O^+ и полученные таким образом группы $\mathfrak{A}_0$ и $\mathfrak{A}$ будем записывать аддитивно. Обозначив через D, D', D'' прямые (соответственно полупрямые с началом 0), будем, по определению, иметь

$$\widehat{(D, D'')} = \widehat{(D, D')} + \widehat{(D', D'')} \quad \text{(теорема Шаля).} \tag{9}$$

Отсюда следуют равенства

$$(\widehat{D, D}) = 0, \quad (\widehat{D, D'}) = -(\widehat{D', D}). \tag{10}$$

Замечания. 1) Множество L прямых (соответственно полупрямых с началом 0) плоскости E является однородным пространством абелевой группы S^+/H (соответственно O^+) таким, что единственный оператор, оставляющий инвариантными все элементы L,— это нейтральный элемент. Следовательно, к пространству L можно применять формулы приложения II, n° 1, гл. II; таким образом, предложение 8 есть частный случай «правила параллелограмма», а формулы (9) и (10) — частные случаи формул (2) (там же).

2) Для определения группы углов между прямыми вместо группы S^+/H можно использовать группу $O^+/\{-1, 1\}$, канонически ей изоморфную (предложение 7). Тогда канонический гомоморфизм группы O^+ на факторгруппу $O^+/\{-1, 1\}$ соответствует некоторому гомоморфизму группы $\mathfrak{A}$ на $\mathfrak{A}_0$, именно гомоморфизму, который углу между каждыми полупрямыми Δ, Δ' ставит в соответствие угол между прямыми D, D', содержащими соответственно Δ и Δ'. °Если A — поле действительных чисел, то группа $\mathfrak{A}$ является *накрытием* порядка 2 группы $\mathfrak{A}_0$.°

В силу предложения 8 все углы между прямыми (соответственно полупрямыми) вида $(\widehat{D', D''})$, где D' и D'' ортогональны (соответственно вида $(\widehat{D, -D})$), равны: в самом деле, это следует из замечания 2 n° 1 (соответственно это очевидно). Этот угол между прямыми (соответственно полупрямыми) называется *прямым* (соответственно *развернутым*) *углом* и является в группе $\mathfrak{A}_0$ (соответственно в группе $\mathfrak{A}$) элементом порядка 2.

Предложение 9. *Пусть A — максимальное упорядоченное поле и Φ — положительная форма. Для любого целого $n > 1$ число элементов ϑ группы $\mathfrak{A}_0$ углов между прямыми* (соответственно *группы $\mathfrak{A}$ углов между полупрямыми*) *таких, что $n\vartheta = 0$, равно n.*

Группы $\mathfrak{A}_0$, S^+/H, $\mathfrak{A}$ и O^+ изоморфны (предложение 3), и поэтому достаточно доказать утверждение только для группы O^+, то есть доказать, что существует ровно n вращений v таких, что $v^n = 1$. Но так как упорядоченное поле A максимально,

а поле A (Ф) — его расширение степени 2 (предложение 1а)), то A (Ф) алгебраически замкнуто (гл. VI, § 2, n° 6, теорема 3). Следовательно, корни степени n из единицы этого поля образуют циклическую группу порядка n (гл. V, § 1, n° 1, теорема 1). Но для любого элемента $u \in A$ (Ф) его норма $N(u) = u\bar{u} \geqslant 0$, так что равенство $u^n = 1$ влечет $N(u) = 1$, и значит, u есть вращение (n° 1, замечание 1). Это и доказывает наше утверждение.

Следствие. *Прямой угол* (соответственно *развернутый угол*) *является единственным элементом порядка* 2 *в группе* $\mathfrak{A}_0$ (соответственно в группе $\mathfrak{A}$).

Наконец, предположим, что плоскость E ориентирована.

Лемма 1. *Пусть* u *— прямое подобие плоскости* E; *все бивекторы вида* $x \wedge u(x)$ *принадлежат одной замкнутой полупрямой из* $\bigwedge^2 E$.

В случае, когда подобие u является гомотетией, утверждение леммы тривиально. В противоположном случае $x \wedge u(x) \neq 0$ для любого $x \neq 0$; пусть x и y — векторы плоскости E, $x \neq 0$, $y \neq 0$; существует подобие $v \in S^+$ такое, что $y = v(x)$, откуда $y \wedge u(y) = v(x) \wedge uv(x) = v(x) \wedge v(u(x)) = (\det v)(x \wedge u(x))$; взяв в плоскости E ортонормальный базис, убедимся, что $\det v$ положителен (предложение 1б)), откуда и следует наше утверждение.

Но если это так, то среди двух образующих w поля A (Ф) таких, что $w^2 = -1$, есть единственный элемент, для которого бивектор $x \wedge w(x)$ положителен при любом $x \in E$. Именно этот образующий мы и выберем для определения функций c_w, s_w и t_w (n° 2). Пусть h и h' — определенные выше канонические биекции группы $\mathfrak{A}_0$ углов между прямыми на группу S^+/H и группы $\mathfrak{A}$ углов между полупрямыми на группу O^+. Отображение $t_w \circ h$ группы $\mathfrak{A}_0$ в проективное поле $\tilde{A}$ и отображения $c_w \circ h'$ и $s_w \circ h'$ группы $\mathfrak{A}$ в поле A обозначаются соответственно tg, cos и sin и называются *тангенс*, *косинус* и *синус*. Отображение $\varphi \to 1/\mathrm{tg}\,\varphi$ группы $\mathfrak{A}_0$ в $\tilde{A}$ обозначается через ctg и называется *котангенсом*. Косинус, синус, тангенс и котангенс называют *тригонометрическими функциями*. Допуская вольность речи, через tg и ctg

обозначают также композиции $\mathrm{tg} \circ p$ и $\mathrm{ctg} \circ p$, где p — канонический гомоморфизм группы $\mathfrak{A}$ на $\mathfrak{A}_0$ (см. выше замечание 2).

Формулы (2), (8), (3), (4), (5) и (7) n° 2 при $\delta = -1$ превращаются в формулы:

$$\mathrm{tg}(\varphi + \varphi') = \frac{\mathrm{tg}\,\varphi + \mathrm{tg}\,\varphi'}{1 - \mathrm{tg}\,\varphi\,\mathrm{tg}\,\varphi'}, \tag{11}$$

$$\mathrm{tg}(2\varphi) = \frac{2\,\mathrm{tg}\,\varphi}{1 - \mathrm{tg}^2\,\varphi} \tag{12}$$

для φ, $\varphi' \in \mathfrak{A}_0$;

$$\cos^2\vartheta + \sin^2\vartheta = 1, \tag{13}$$

$$\cos(\vartheta + \vartheta') = \cos\vartheta\cos\vartheta' - \sin\vartheta\sin\vartheta', \tag{14}$$

$$\sin(\vartheta + \vartheta') = \sin\vartheta\cos\vartheta' + \cos\vartheta\sin\vartheta', \tag{15}$$

$$\begin{cases} \sin(2\vartheta) = \dfrac{2\,\mathrm{tg}\,\vartheta}{1 + \mathrm{tg}^2\,\vartheta}, \\ \cos(2\vartheta) = \dfrac{1 - \mathrm{tg}^2\,\vartheta}{1 + \mathrm{tg}^2\,\vartheta} \end{cases} \tag{16}$$

для ϑ, $\vartheta' \in \mathfrak{A}$. Кроме того, из определений или из предыдущих формул легко следуют формулы:

$$\mathrm{tg}\,\vartheta = \frac{\sin\vartheta}{\cos\vartheta}, \qquad \mathrm{ctg}\,\vartheta = \frac{\cos\vartheta}{\sin\vartheta}, \tag{17}$$

$$1 + \mathrm{tg}^2\,\vartheta = \frac{1}{\cos^2\vartheta}, \qquad 1 + \mathrm{ctg}^2\,\vartheta = \frac{1}{\sin^2\vartheta} \tag{18}$$

для $\vartheta \in \mathfrak{A}$.

Углом между двумя ненулевыми векторами x, y плоскости E, взятыми в данном порядке, называется угол между полупрямыми, содержащими эти векторы; этот угол обозначается $\widehat{(x, y)}$. Для любого вектора $x \in E$ его *длиной* называется элемент $\Phi(x, x)^{1/2}$ поля A; длина вектора обозначается $|x|$.

Предложение 10. *Пусть A — максимальное упорядоченное поле. Предположим, что плоскость E ориентирована и форма Φ положительна. Для любой пары ненулевых векторов x, y плоскости E выполняются равенства*

$$\cos\widehat{(x, y)} = \frac{\Phi(x, y)}{|x|\,|y|}, \tag{19}$$

$$\sin\widehat{(x, y)} \cdot e = \frac{x \wedge y}{|x|\,|y|}, \tag{20}$$

где e — положительный бивектор такой, что $\Phi_{(2)}(e, e) = 1$.

В самом деле, векторы $x' = x/|x|$ и $y' = y/|y|$ имеют длину 1, следовательно, существует единственное вращение v такое, что $v(x') = y'$ (n° 1, следствие 2 предложения 1). Положив $v = a + bw$ $(a, b \in A)$, получим, по определению, $a = \cos\widehat{(x, y)}$ и $b = \sin\widehat{(x, y)}$. Равенство $y' = v(x') = ax' + bw(x')$ влечет $\Phi(x', y') = a\Phi(x', x') = a$, так как x' и $w(x')$ ортогональны (замечание 2 n° 1), что доказывает равенство (19). С другой стороны, по определению продолжения $\Phi_{(2)}$ формы Φ на внешнюю степень $\overset{2}{\bigwedge} E$ (§ 1, n° 9, формула (37)) и по выбору элемента w, из этого соотношения следует также, что $x' \wedge y' = bx' \wedge w(x') = be$, что доказывает равенство (20).

Замечания. 3) Пусть в *аффинной плоскости* L, ассоциированной с плоскостью E, заданы две прямые (соответственно полупрямые) D, D'. Углом между этими прямыми называется угол, образованный их направляющими прямыми в плоскости E (соответственно полупрямыми с началом 0 плоскости E, соответствующими прямым D и D') (гл. II, приложение II, n° 1 и n° 3); угол между прямыми D и D' обозначается $\widehat{(D, D')}$.

4) Пусть F — векторное пространство *произвольной* размерности над максимальным упорядоченным полем A, и Ψ — невырожденная положительная симметрическая билинейная форма на пространстве F, и пусть F' — векторная плоскость, порожденная двумя заданными линейно независимыми векторами x, y; *углом* между векторами x и y называется угол между этими векторами, как элементами плоскости F'; этот угол обозначается $\widehat{(x, y)}$. По формуле (19) косинус этого угла равен

$$\cos\widehat{(x, y)} = \frac{\Phi(x, y)}{|x|\,|y|} \tag{21}$$

(где число $|x| = \Psi(x, x)^{1/2}$ также называется *длиной* вектора x) и, следовательно, *не зависит от выбора ориентации* на плоскости F'. Функции синус и тангенс угла $\widehat{(x, y)}$ при изменении ориента-

ции плоскости F' меняют знак. Если ненулевые векторы x и y пространства F пропорциональны, то угол $\overset{\frown}{(x, y)}$ считают равным нулю.

4. *Угловые секторы*

Будем сначала предполагать только, что E — *ориентированная* плоскость над *упорядоченным* полем A. Будем говорить, что три полупрямые D_0, D_1, D_2 (с началом 0) плоскости E образуют направленную последовательность, если для $x_i \in D_i$, $x_i \neq 0$ ($i = 1, 2, 3$), по меньшей мере два из бивекторов $x_0 \wedge x_1$, $x_1 \wedge x_2$, $x_2 \wedge x_0$ строго положительны; в этом случае последовательности D_1, D_2, D_0 и D_2, D_0, D_1 также будут направленными. Ясно, что любые три прямые, образующие направленную последовательность, различны между собой. Пусть D_1 и D_2 — произвольные полупрямые плоскости E. *Открытым* (соответственно *замкнутым*) *угловым сектором* с началом D_1 и концом D_2 называется множество (или, более вольно, объединение) всех полупрямых D таких, что последовательность D_1, D, D_2 направленная (соответственно таких, что $D = D_1$, или $D = D_2$, или последовательность D_1, D, D_2 направленная).

Предложение 11. *Пусть E — ориентированная плоскость над упорядоченным полем A, D_0 — полупрямая в плоскости E, G — множество полупрямых, отличных от D_0. Отношение*

«$D_1 = D_2$ или последовательность D_0, D_1, D_2 направленная»

между элементами D_1 и D_2 множества G является отношением совершенного порядка в множестве G'.

В самом деле, все аксиомы отношения строгого порядка, кроме транзитивности, проверяются тривиально. Пусть D_1, D_2, D_3 — три прямые такие, что последовательности D_0, D_1, D_2 и D_0, D_2, D_3 направленные. Покажем, что последовательность D_0, D_1, D_3 также направленная. Для этого возьмем на полупрямой D_i ($i = 0, 1, 2, 3$) вектор $x_i \neq 0$, выберем некоторый бивектор $e > 0$ и положим $x_i \wedge x_j = a_{ij}e$ ($a_{ij} \in A$).

Записав бивектор e в виде $x_0 \wedge y$ ($y \in E$) и взяв (x_0, y) в качестве базиса плоскости E, легко получить соотношение

$$a_{01}a_{23} + a_{02}a_{31} + a_{03}a_{12} = 0. \tag{22}$$

Но тогда, если $a_{01} \leqslant 0$, то $a_{12} > 0$ и $a_{20} > 0$ (так как первая последовательность направленная), далее, $a_{23} > 0$ и $a_{30} > 0$ (так как $a_{02} < 0$ и вторая последовательность направленная); отсюда по формуле (22) $a_{13} > 0$; следовательно, в данном случае последовательность D_0, D_1, D_3 направленная. Пусть теперь $a_{01} > 0$. Если $a_{30} \leqslant 0$, то $a_{02} > 0$ и $a_{23} > 0$ (так как вторая последовательность направленная); далее, $a_{12} > 0$ (так как $a_{20} < 0$ и первая последовательность направленная); отсюда по формуле (22) $a_{13} > 0$, то есть последовательность D_0, D_1, D_3 направленная. Наконец, в случае $a_{01} > 0$ и $a_{30} > 0$ утверждение очевидно.

Следствие. *Пусть D_1 и D_2 — две различные полупрямые плоскости E. Для любой полупрямой D_0 плоскости E, такой, что последовательность D_0, D_1, D_2 направленная, множество полупрямых плоскости E, удовлетворяющих условиям $D_1 < D < D_2$ (в смысле отношения совершенного порядка, определяемого полупрямой D_0), совпадает с открытым угловым сектором с началом D_1 и концом D_2.*

В самом деле, требуется доказать, что отношения «последовательность D_1, D_3, D_2 направленная» и «последовательности D_0, D_1, D_3 и D_0, D_3, D_2 направленные» эквивалентны. Обозначим для краткости через (ijk) отношение «последовательность D_i, D_j, D_k направленная». По предложению 11 конъюнкция отношений (132) и (120) влечет (130); аналогично конъюнкция отношений (201) и (213) влечет (203), и в одну сторону утверждение доказано.

Обратно, предположим, что выполнены отношения (012), (013), (032); тогда конъюнкция отношений (312) и (320) влечет (310) (предложение 11), а (310) и (013) несовместимы, поэтому отношение (312) не выполняется. Поэтому справедливо отношение (132), что и заканчивает доказательство.

В соответствии с этим следствием открытый (соответственно замкнутый) угловой сектор с началом D_1 и концом D_2 обозначают через $]D_1, D_2[$ (соответственно $[D_1, D_2]$), подразумевая при этом, что речь идет об *интервале* для структуры порядка, определенной любой прямой D_0 такой, что последовательность D_0, D_1, D_2 направленная.

Предложение 12. *Пусть A — максимальное упорядоченное поле, E — ориентированная плоскость над полем A, D_0 — полупрямая в плоскости E, и G — множество отличных от D_0 полупрямых плоскости E. Совершенно упорядоченные множества A и G изоморфны.*

В самом деле, возьмем в плоскости E такой базис (x, y), что $x \in -D_0$ и бивектор $x \wedge y > 0$. Каждому элементу $t \in A$ поставим в соответствие полупрямую $f(t)$, содержащую вектор $(1 - t^2)\,x + 2ty$. Яснее, $f(A) \subset G$. Покажем, что отображение f *строго возрастающее*. В самом деле, для того чтобы последовательность D_0, $f(t)$, $f(t')$ $(t, t' \in A)$ была направленной, необходимо и достаточно, по определению, чтобы по крайней мере два из элементов

$$-2t,\ (1-t^2)\,2t' - (1-t'^2)\,2t,\ 2t'$$

были >0. Но второй элемент равен $2(t' - t)(1 + tt')$, так что при $t < t'$ имеем: если $tt' \geqslant 0$, то $t' > 0$ или $-t > 0$, а если $tt' < 0$, то $-t > 0$ и $t' > 0$; во всех случаях последовательность D_0, $f(t)$, $f(t')$ направленная. Так как множество A совершенно упорядочено, то отображение f является изоморфизмом множества A на $f(A)$ (Теор. мн., гл. III, § 1, n° 14, предложение 13).

Остается доказать, что отображение f *сюръективно*. Рассмотрим для этого на плоскости E такую положительную форму Ф, чтобы базис (x, y) был ортонормальным относительно Ф. Для всякой полупрямой $D \in G$ существует единственный угол φ такой, что $2\varphi = (\widehat{-D_0,\ D})$ (n° 1, предложение 1); так как угол $(\widehat{-D_0,\ D})$ не является развернутым, то угол φ не будет прямым и, следовательно, $\operatorname{tg}\varphi$ конечен. По формулам (16) (n° 3) $D = f(\operatorname{tg}\varphi)$, что и заканчивает доказательство.

Упражнения. 1) В обозначениях n° 1 положим $Q(x) = \Phi(x, x)$. Векторное пространство E канонически отождествляется с $C^-(Q)$ (§ 9, n° 1). Для любых элементов $z \in C^+(Q)$ и $x \in E$ имеем $zx \in E$; показать, что $s_z : x \to zx$ принадлежит группе $A(\Phi)$ и отображение $z \to s_z$ является изоморфизмом алгебры $C^+(Q)$ на $A(\Phi)$.

2) Обозначения и предположения те же, что в n° 1 и упражнении 1.

а) Пусть C — множество таких элементов $x \in E$, что $\Phi(x, x) = 1$ («единичная окружность»), и $\mathfrak{D}$ — множество прямых D, пересечение которых с C не пусто (и, следовательно, состоит из двух про-

тивоположных элементов E). *Прямой с отмеченной точкой* называется всякая пара (D, z), состоящая из некоторой прямой $D \in \mathfrak{D}$ и точки $z \in D \cap C$. Показать, что для любых двух прямых с отмеченной точкой $\Delta_1 = (D_1, z_1)$ и $\Delta_2 = (D_2, z_2)$ существует единственное вращение u такое, что $u(z_1) = z_2$ (и, следовательно, $u(D_1) = D_2$); этот факт будем выражать равенством $u(\Delta_1) = \Delta_2$. Определенное на множестве пар (Δ_1, Δ_2) прямых с отмеченной точкой отношение «существует вращение u такое, что $u(\Delta_1) = \Delta_1'$ и $u(\Delta_2) = \Delta_2'$» является отношением эквивалентности. Множество классов эквивалентности прямых с отмеченной точкой по этому отношению называется множеством *углов между прямыми с отмеченными точками*, и класс эквивалентности, в котором лежит некоторая пара (Δ_1, Δ_2) прямых с отмеченными точками, называется *углом*, образуемым этой парой, и обозначается $\widehat{(\Delta_1, \Delta_2)}$; отношение $\widehat{(\Delta_1, \Delta_2)} = \widehat{(\Delta_1', \Delta_2')}$ эквивалентно $\widehat{(\Delta_1, \Delta_1')} = \widehat{(\Delta_2, \Delta_2')}$, и вращение, переводящее Δ_1 в Δ_2, называется *вращением на угол* $\vartheta = \widehat{(\Delta_1, \Delta_2)}$ и обозначается $h_1(\vartheta)$; h_1 является биекцией множества $\mathfrak{A}_1$ на O^+; посредством отображения h_1^{-1} на множество $\mathfrak{A}_1$ переносится структура коммутативной группы O^+; таким образом определенная группа $\mathfrak{A}_1$ записывается аддитивно; *развернутым* углом в $\mathfrak{A}_1$ называется угол, образованный прямой с отмеченной точкой (D, z) и прямой с «противоположно» отмеченной точкой $(D, -z)$, который соответствует вращению $x \to -x$.

б) На множестве $\mathfrak{D}_0 \supset D$ неизотропных прямых, так же как в n° 3, определяются понятия *угла между прямыми*, группы $\mathfrak{A}_0$ (используется следствие 3 предложения 1 n° 1), *прямого* угла в $\mathfrak{A}_0$ и канонической биекции h группы $\mathfrak{A}_0$ на S^+/H. Положим в обозначениях следствия предложения 3 $\overline{d} = h_1^{-1} \circ d \circ h$ и $\overline{i} = h^{-1} \circ i \circ h_1$; тогда $\overline{i}$ — гомоморфизм группы $\mathfrak{A}_1$ в $\mathfrak{A}_0$, $\overline{d}$ — гомоморфизм группы $\mathfrak{A}_0$ в $\mathfrak{A}_1$; гомоморфизм $\overline{d}$ биективен, ядро гомоморфизма $\overline{i}$ состоит из нуля и развернутого угла; кроме того, $\overline{d}(\overline{i}(\vartheta)) = 2\vartheta$ для $\vartheta \in \mathfrak{A}_1$ и $\overline{i}(\overline{d}(\varphi)) = 2\varphi$ для $\varphi \in \mathfrak{A}_0$. Гомоморфизм $\overline{i}$ сюръективен (другими словами, $\mathfrak{D}$ совпадает со множеством всех неизотропных прямых) тогда и только тогда, когда поле A пифагорово (гл. VI, § 2, упражнение 8г)) и существует базис, ортонормальный относительно формы Φ; вместе с тем элемент $\Phi(x, x)$ при любом $x \in E$ является *квадратом*.

3) Обозначения и предположения те же, что в упражнении 2.

а) Пусть s — симметрия относительно неизотропной прямой D (§ 6, n° 4). Для всякой прямой с отмеченной точкой $\Delta_1 = (D_1, z_1)$ положим

$$\Delta_2 = s(\Delta_1) = (s(D_1), s(z_1)),$$

и пусть $\varphi = \widehat{(D_1, D)}$; показать, что $\widehat{(\Delta_1, \Delta_2)} = \overline{d}(\varphi)$.

б) Показать, что всякое ортогональное преобразование с определителем -1 является симметрией s относительно некоторой неизотропной прямой (см. § 6, упражнение 15д)); для всякого вращения u имеем равенство $sus^{-1} = u^{-1}$.

в) Для любых двух точек $x, y \in E$, таких, что $\Phi(x, x) = \Phi(y, y) \neq 0$, существует единственная симметрия относительно некоторой неизотропной прямой, переводящая x в y.

г) Пусть s, s' — симметрия относительно неизотропных прямых D, D' и $\varphi = (\widehat{D, D'})$; для того чтобы произведение $s's$ было вращением с углом ϑ, необходимо и достаточно, чтобы $\overline{d}(\varphi) = \vartheta$.

д) Показать, что коммутант ортогональной группы $\boldsymbol{O}(Q)$ является образом группы $\mathfrak{A}_1$ при гомоморфизме $\vartheta \to h_1(2\vartheta)$ (§ 6, упражнение 17а)); этот образ совпадает с O^+ тогда и только тогда, когда гомоморфизм $\overline{i}$ сюръективен (упражнение 2б)).

4) Обозначения и предположения те же, что в упражнении 2. Пусть a, b — две точки окружности C, Δ_a, Δ_b — прямые с отмеченными точками, проходящие соответственно через a и b (и через 0), и $\vartheta = (\widehat{\Delta_a, \Delta_b})$. Для всякой точки $x \in E$, отличной от a и b, через D_{xa} (соответственно D_{xb}) обозначим аффинную прямую, проходящую через a и x (соответственно через b и x); пусть D'_{xa} (соответственно D'_{xb}) — направляющая прямая D_{xa} (соответственно D_{xb}); показать, что $x \in C$ (точка x отлична от a и b) тогда и только тогда, когда угол $\varphi = (\widehat{D'_{xa}, D'_{xb}})$ удовлетворяет условию $\overline{d}(\varphi) = \vartheta$ (воспользоваться упражнением 3). Как изменится это утверждение в случае $x = a$ или $x = b$ (см. упражнение 25а) § 6)?

5) В обозначениях n°n° 1 и 2 и упражнения 2 предположим, что Φ — форма индекса 1, иными словами, δ есть квадрат γ^2 в поле A; обозначим через D_1, D_2 изотропные прямые плоскости E, содержащие соответственно векторы $e_1 - \frac{1}{\gamma} e_2$ и $e_1 + \frac{1}{\gamma} e_2$.

а) Показать, что группа вращений $\boldsymbol{O}^+$ изоморфна мультипликативной группе A^* поля A.

б) Для всякого угла $\vartheta \in \mathfrak{A}_1$ положим $e_w(\vartheta) = c_w(h_1(\vartheta)) + \gamma s_w(h_1(\vartheta))$. Показать, что отображение $\vartheta \to e_w(\vartheta)$ есть изоморфизм группы $\mathfrak{A}_1$ на группу A^*.

в) Пусть D, D' — произвольные прямые и $\varphi = (\widehat{D, D'})$. Показать, что двойное отношение $\begin{bmatrix} D_1 & D_2 \\ D' & D \end{bmatrix}$ (гл. II, приложение III, упражнение 5) равно $e_w(\overline{d}(\varphi))$ («*формула Лагерра*»). (Заметить, что прямые D_1 и D_2 инвариантны относительно всех прямых подобий, и, пользуясь упражнением 4в) гл. II, приложение III, свести доказательство к случаю $D = Ae_1$.)

6) Предположим, что поле A упорядочено.

а) Пусть D_1, D_2 — неизотропные полупрямые с началом 0. Показать, что существует прямое подобие u такое, что $u(D_1) = D_2$; всякое подобие, обладающее этим свойством, имеет вид $v = su$, где s — гомотетия с коэффициентом > 0.

б) Определенное на множестве пар (D_1, D_2) неизотропных полупрямых отношение «существует прямое подобие u такое, что $u(D_1) = D_1'$ и $u(D_2) = D_2'$» есть отношение эквивалентности. Множество классов эквивалентности неизотропных полупрямых по этому отношению называется множеством *углов между полупрямыми* (неизотропными), и класс эквивалентности, в котором лежит некоторая пара (D_1, D_2) таких полупрямых, называется *углом*, образованным этой парой, и обозначается $\widehat{(D_1, D_2)}$, угол $\vartheta = \widehat{(D_1, D_2)}$ называют *углом* всякого прямого подобия, переводящего D_1 в D_2; пусть $h_2(\vartheta)$ — класс этих подобий по mod H; тогда h_2 является биекцией множества $\mathfrak{A}$ на группу S^+/H^+; посредством отображения h_2^{-1} на множество $\mathfrak{A}$ переносится структура коммутативной группы S^+/H^+; определенная таким образом группа обозначается аддитивно. Определить каноническую инъекцию $\bar{j}$ группы $\mathfrak{A}_1$ углов между прямыми с отмеченными точками (упражнение 2) в группу $\mathfrak{A}$ таким образом, чтобы отображение $h_2 \circ j \circ h_2^{-1}$ было канонической инъекцией j группы O^+ в S^+/H^+. Отображение $\bar{j}$ сюръективно тогда и только тогда, когда сюръективен гомоморфизм $\bar{i}$ группы $\mathfrak{A}_1$ в $\mathfrak{A}_0$ (упражнение 2б)).

в) Показать, что уравнение $2\vartheta = 0$ в группе $\mathfrak{A}$ имеет два решения при $\delta < 0$ и четыре решения при $\delta > 0$. В первом случае решение $\omega \neq 0$ этого уравнения также называется *развернутым* углом.

*7) Сохраняя предположения и обозначения упражнения 6, будем считать, что гомоморфизм $\bar{j}$ биективен; тогда для любого $\vartheta \in \mathfrak{A}$ можно определить $\cos\vartheta$ и $\sin\vartheta$ так же, как в n° 3. Пусть T — множество таких $\vartheta \in \mathfrak{A}$, что $\sin\vartheta \geqslant 0$.

а) Показать, что для всякого угла $\vartheta \in T$ существует единственный угол $\vartheta' \in T$ такой, что $2\vartheta' = \vartheta$; положим $\vartheta' = \vartheta/2$.

б) Пусть L — $\boldsymbol{Z}$-модуль формальных линейных комбинаций множества T с коэффициентами из $\boldsymbol{Z}$ (гл. II, § 1, n° 8); обозначим через $\xi \dot{+} \eta$ и $\dot{-}\xi$ сумму и противоположный элемент в L. Пусть N — подмодуль L, порожденный элементами вида $\xi \dot{+} \eta \dot{-} (\xi + \eta)$ для всех пар (ξ, η) элементов T таких, что $\xi + \eta \in T$ (сумма взята в группе $\mathfrak{A}$). Пусть $\dot{f}$ — гомоморфизм модуля L в $\mathfrak{A}$, являющийся продолжением канонической инъекции множества T в $\mathfrak{A}$, и $\dot{g}$ — эндоморфизм модуля L, продолжающий отображение $\vartheta \to \vartheta/2$ множества T в себя. Тогда $\dot{f}(N) = \{0\}$ и $\dot{g}(N) \subset N$. Путем факторизации из гомоморфизма $\dot{f}$ получается гомоморфизм f модуля $M = L/N$ в $\mathfrak{A}$, а из $\dot{g}$ —

эндоморфизм модуля M; положим $g(\mu) = \mu/2$; тогда $g^m(\mu) = 2^{-m}\mu$, где g^m — итерированная m-я степень g; имеем равенство $2^m(2^{-m}\mu) = \mu$ для любого $\mu \in M$.

в) Показать, что сужение на T канонического отображения ψ модуля L на $M = L/N$ инъективно; это позволяет посредством ψ отождествить T с некоторым подмножеством модуля M. Показать, что сумма $\lambda_1 + \lambda_2 + \ldots + \lambda_m$ ненулевых элементов $\lambda_1, \lambda_2, \ldots, \lambda_m$ множества T не может быть равна нулю в M (рассмотреть элемент $2^{-m}(\lambda_1 + \ldots + \lambda_m)$ и применить индукцию по m, заметив, что эти элементы принадлежат T).

г) Пусть M_+ — множество конечных сумм (в M) элементов множества T; показать, что $M_+ \cap (-M_+) = \{0\}$ и $M = M_+ \cup (-M_+)$ и, следовательно, M_+ является множеством элементов $\geqslant 0$ в некоторой структуре *совершенно упорядоченной группы*, определенной на M (заметить, что для любого $\mu \in M_+$ существует целое число m такое, что $2^{-m}\mu \in T$); эта совершенно упорядоченная группа называется *группой мер углов между полупрямыми*. Показать, что гомоморфизм f модуля M в $\mathfrak{A}$ сюръективен и его ядро есть множество целых кратных угла 2ω, где ω — развернутый угол (упражнение 6в)). Доказать, что множество T отождествляется с интервалом $[0, \omega]$ в M (индукцией по m установить, что если $\mu, \lambda_1, \ldots, \lambda_m$ принадлежат T и $\lambda_1 + \ldots + \lambda_m \leqslant \mu$, то $\lambda_1 + \ldots + \lambda_m \in T$). Показать, что функция $\vartheta \to \cos\vartheta$, определенная на множестве T (отождествленном с интервалом в M), строго убывающая.

д) Для того чтобы совершенно упорядоченная группа M была архимедовой (гл. VI, § 1, упражнение 31), необходимо и достаточно, чтобы аддитивная группа поля A была архимедовой. (Для доказательства необходимости заметить, что если $\sin\vartheta$ бесконечно мал относительно подполя $\boldsymbol{Q}$ поля A (гл. VI, § 2, упражнение 1), то $\sin n\vartheta$ для любого n тоже бесконечно мал. Для доказательства достаточности заметить, что при $0 \leqslant \vartheta \leqslant \omega/4$ справедливо неравенство $\sin 2\vartheta \geqslant \geqslant \sqrt{2}\sin\vartheta$.)

8) Пусть E — ориентированная плоскость над упорядоченным полем A, D', D'' — различные полупрямые, x' (соответственно x'') — отличный от нуля вектор на D' (соответственно D''). Угловой сектор с началом D' и концом D'' называется *меньшим развернутого* (соответственно *большим развернутого*, *развернутым*), если $x' \wedge x'' > 0$ (соответственно $x' \wedge x'' < 0$, $x' \wedge x'' = 0$).

а) Для существования автоморфизма векторного пространства E, переводящего открытый (соответственно замкнутый) угловой сектор Σ_1 в открытый (соответственно замкнутый) сектор Σ_2, необходимо и достаточно, чтобы секторы Σ_1 и Σ_2 были или оба меньше развернутого, или оба больше развернутого, или оба развернутыми.

б) Показать, что упорядоченное множество $[D', D'']$ изоморфно интервалу $[0, 1]$ поля A (рассмотреть сначала случай, когда сектор

меньше развернутого, и заметить, что любые два ограниченных интервала поля A изоморфны, как упорядоченные множества).

в) В обозначениях и предположениях упражнения 7 определить каноническое биективное отображение множества T на развернутый угловой сектор и показать, что это отображение является изоморфизмом для структуры порядка.

9) Пусть A — пифагорово упорядоченное поле, E — конечномерное векторное пространство над полем A, Q — невырожденная положительная квадратичная форма на E, относительно которой пространство E имеет ортонормальный базис (иными словами, $Q(x)$ является в поле A квадратом при любом $x \in E$) Показать, что коммутант $\Omega(Q)$ ортогональной группы $\boldsymbol{O}(Q)$ есть группа вращений $\boldsymbol{O}^+(Q) = \boldsymbol{SO}(Q)$ (использовать упражнение 3а) § 10 и упражнение 17а) § 6).

10) Пусть A — максимальное упорядоченное поле, E — конечномерное векторное пространство над A, Q — невырожденная положительная квадратичная форма на E. Показать, что для всякого ортогонального преобразования $u \in \boldsymbol{O}(Q)$ существует разложение пространства E в прямую сумму попарно ортогональных подпространств P, N, R_i $(1 \leqslant i \leqslant r)$, обладающих следующими свойствами: 1° $u(x) = x$ в P, $u(x) = -x$ в N; 2° каждое подпространство R_i имеет размерность 2, $u(R_i) = R_i$ и сужение преобразования u на R_i есть вращение на угол ϑ_i, отличный от нуля и развернутого угла. Кроме того, для любых двух таких разложений подпространства P и N, так же как и последовательности элементов $\cos\vartheta_i$, с точностью до порядка совпадают (см. § 7, n° 3, следствие 2 теоремы 2). Вывести отсюда, что всякое вращение $u \in \boldsymbol{O}^+(Q)$ является коммутатом $tst^{-1}s^{-1}$, где s и t — элементы группы $\boldsymbol{O}(Q)$ и $s^2 = 1$ (см. упражнение 3г)).

11) Пусть A — максимальное упорядоченное поле, L — тело кватернионов над полем A (соответствующее паре $(-1, -1)$), E — подпространство (размерности 3), состоящее из чистых кватернионов L (§ 9, упражнение 15а)); всякий кватернион единственным образом может быть тогда записан в виде $s = \alpha \cdot 1 + v$, где $\alpha \in A$, $v \in E$; при этом $\alpha^2 - v^2 = \varrho \cdot 1$, где $\varrho \in A$, $\varrho \geqslant 0$; положим $\| v \| = \sqrt{\varrho}$.

а) Пусть $\varphi(s)$ — вращение $x \to sxs^{-1}$ пространства E относительно невырожденной положительной квадратичной формы $x \to \| x \|^2$ на пространстве E (§ 9, n° 5, теорема 4 и упражнение 15). Показать, что если $v \neq 0$, то векторы прямой $D \subset E$, содержащей кватернион v, инвариантны относительно $\varphi(s)$; сужение вращения $\varphi(s)$ на ортогональную к D плоскость $P = D^0$ является вращением на угол ϑ, причем (при соответствующей ориентации пространства P) $\operatorname{tg}\dfrac{\vartheta}{2} = \| v \| / \alpha$. (Пусть $(1, i, j, k)$ — канонический базис тела L над полем A; свести доказательство к случаю, когда $v = \beta i$, $\beta \in A$, и вычислить sjs^{-1}.)

б) Показать, что всякий кватернион с нормой 1 может быть представлен в виде $tst^{-1}s^{-1}$, где $s \in L$, $t \in E$ (см. упражнение 10), и для любых чистых кватернионов a и b с нормой 1 существует кватернион s такой, что $b = sas^{-1}$.

в) Кватернионы $s = \alpha + v$, $t = \beta + w$, где $\alpha, \beta \in A$, $v, w \in E$, перестановочны тогда и только тогда, когда $v = \lambda w$, $\lambda \in A$; $st = -ts$ тогда и только тогда, когда $\alpha = \beta = 0$, и векторы v и w ортогональны (см. § 3, упражнение 10).

12) Пусть A — максимальное упорядоченное поле, L — евклидово пространство над A размерности n, и его метрическая форма Φ невырождена и положительна; обозначим через $d(x, y)$ расстояние $\sqrt{\Phi(x-y, x-y)}$ между двумя точками L (§ 7, п° 1, замечание). *Сферой радиуса* ϱ *с центром в точке* c, где $c \in L$ и $\varrho > 0$ — элемент поля A, называется множество таких $x \in L$, что $d(x, c) = \varrho$; таким образом, сферы являются невырожденными аффинными квадриками в L, имеющими центр (§ 6, упражнение 25).

а) Пусть x — точка сферы с центром в точке c. Показать, что гиперплоскость, касательная к сфере S в точке x (§ 6, упражнение 25), перпендикулярна (§ 6, упражнение 22) к прямой, проходящей через c и x.

б) Пусть S — сфера радиуса ϱ с центром в точке c, a — точка L, D — прямая, проходящая через точку a и пересекающая сферу S в двух различных точках x_1, x_2 (соответственно касательная к S в точке x). Доказать равенства

$$\Phi(x_1 - a, x_2 - a) = (d(a, c))^2 - \varrho^2$$

(соответственно $(d(x, a))^2 = (d(a, c))^2 - \varrho^2$).

Элемент $(d(a, c))^2 - \varrho^2$ поля A называется *степенью* точки a относительно сферы S.

в) Пусть S_1, S_2 — сферы, имеющие различные центры; показать, что множество точек пространства L, имеющих одинаковую степень относительно S_1 и S_2, образует гиперплоскость, перпендикулярную к прямой, проходящей через центры этих сфер, и содержащую пересечение $S_1 \cap S_2$; эта гиперплоскость называется *радикальной гиперплоскостью* сфер S_1 и S_2.

г) Пусть S_1 и S_2 — сферы радиусов соответственно ϱ_1 и ϱ_2 с центрами соответственно в точках c_1 и c_2. Показать, что следующие свойства эквивалентны:

α) Пересечение $S_1 \cap S_2$ не пусто, и гиперплоскости, касательные к S_1 и S_2 в любой точке из этого пересечения, перпендикулярны;

β_1) степень точки c_1 относительно S_2 равна ϱ_1^2;

β_2) степень точки c_2 относительно S_1 равна ϱ_2^2;

γ_1) радикальная гиперплоскость сфер S_1 и S_2 есть полярная гиперплоскость (§ 6, упражнение 25) точки c_1 относительно S_2;

γ_2) радикальная гиперплоскость сфер S_1 и S_2 есть полярная гиперплоскость точки c_2 относительно S_1.

В случае, когда эти условия выполняются, сферы S_1 и S_2 называются *ортогональными*.

д) Пусть c_1, c_2 — центры ортогональных сфер S_1, S_2 и ω_1, ω_2 — степени некоторой точки x относительно S_1 и S_2 соответственно. Показать, что $\omega_1 + \omega_2 = 2\Phi(x - c_1, x - c_2)$. Доказать обратное утверждение.

13) Обозначения и предположения те же, что в упражнении 12. Пусть c — некоторая точка L, $\alpha \neq 0$ — элемент поля A. *Инверсией степени* α *с полюсом* c называется инволютивная подстановка u на множестве $L - \{c\}$ такая, что при любом $x \in L - \{c\}$ элемент $u(x)$ лежит на прямой, проходящей через точки c и x, и удовлетворяет условию $\Phi(x - c, u(x) - c) = \alpha$. Допуская вольность речи, говорят, что u — инверсия в пространстве L.

а) Пусть u, v — инверсии степени α и β с общим полюсом c. Тогда uv^{-1} является сужением на $L - \{c\}$ гомотетии (гл. II, приложение III, упражнение 6) с коэффициентом $\alpha\beta^{-1}$ и центром c.

б) Пусть S — сфера (упражнение 12), содержащая точку c. Показать, что образ множества $S - \{c\}$ при инверсии с полюсом c есть гиперплоскость, перпендикулярная к прямой, соединяющей точку c с центром сферы S. (Допуская вольность речи, говорят, что эта гиперплоскость есть образ S при рассматриваемой инверсии.) Доказать обратное утверждение.

в) Пусть сфера S не содержит точки c, ω — степень точки c относительно S (упражнение 12б)); показать, что образ множества S при инверсии степени α с полюсом c является образом S при гомотетии с коэффициентом α/ω и с центром в точке c. Если $n = 2$, то для всякого $x \in S$ через T (соответственно T') обозначим касательную к S (соответственно к $u(S)$) в точке x (соответственно $u(x)$), а через D — прямую, проходящую через c, x и $u(x)$; показать, что $(\widehat{D, T}) = (\widehat{T', D})$.

г) Пусть S_1, S_2 — ортогональные сферы (упражнение 12г)), S_1', S_2' — образы этих сфер при инверсии с полюсом c. Показать, что если точка c не принадлежит ни S_1, ни S_2, то сферы S_1' и S_2' ортогональны. Если $c \in S_1$ и $c \overline{\in} S_2$, то S_1' — гиперплоскость, содержащая центр сферы S_2'. Если $c \in S_1 \cap S_2$, то S_1' и S_2' — перпендикулярные гиперплоскости (§ 6, упражнение 22). Доказать обратные утверждения.

д) Пусть u — инверсия степени $\alpha = \varrho^2 > 0$ с полюсом c, и C — сфера радиуса ϱ с центром c, x_1, x_2 — точки, лежащие на прямой, проходящей через точку c, отличные от c. Следующие утверждения эквивалентны: α) x_1 и x_2 переводятся один в другой инверсией u; β) x_1 и x_2 сопряжены относительно сферы C (§ 6, упражнение 25); γ) всякая сфера, содержащая точки x_1 и x_2, ортогональна к c. Инверсию u называют также *инверсией сферы* C.

*14) Сохраняя обозначения и предположения упражнения 12, примем 0 за начало в L. Пусть векторное пространство E_1 — прямая сумма пространства L и некоторого пространства Af_1 размерности 1, обозначим через Q_1 квадратичную форму на пространстве E_1, определенную равенством

$$Q_1(x+\eta f_1)=Q(x)+\eta^2$$

для любых $x \in L$ и $\eta \in A$; форма Q_1 положительна и невырождена; пусть C — сфера в E_1 радиуса 1 с центром 0 (относительно Q_1).

Пусть s — инверсия степени 2 с полюсом $-f_1$ евклидова пространства E_1 (упражнение 13); ее сужение s_0 на L переводит L в $C - \{-f_1\}$; допуская вольность речи, s_0 (соответственно s_0^{-1}) называют *стереографической проекцией* пространства L на C (соответственно сферы C на L) *с точки обзора* $-f_1$. Для всякой инверсии u в L с полюсом c отображение $s_0 u s_0^{-1}$ является инволютивной подстановкой на дополнении C множества $\{s_0(c), -f_1\}$; положив $u'(s_0(c)) = -f_1$, $u'(-f_1) = s_0(c)$, ее можно продолжить до инволютивной подстановки u' множества C; подстановка u' называется *инверсией* в C. Аналогично для всякой симметрии v в L относительно некоторой гиперплоскости отображение $s_0 v s_0^{-1}$ является инволютивной подстановкой на дополнении в C множества $\{-f_1\}$; положив $v'(-f_1) = -f_1$, эту подстановку можно продолжить до инволютивной подстановки v' на C; подстановка v' называется *симметрией* в C. Группа подстановок на множестве C, порожденная инверсиями и симметриями, называется *конформной группой* сферы C (или, допуская вольность речи, пространства L).

а) Показать, что конформная группа сферы C порождается симметриями v' и инверсиями u', соответствующими инверсиям в L степени >0. (Использовать упражнение 13 а) и заметить, что в пространстве L всякий перенос, а также гомотетия $x \to -x$ являются произведениями симметрий относительно гиперплоскостей.)

б) Пусть u — инверсия в L степени >0 и u' — соответствующая инверсия в C; показать, что u' является сужением на C однозначно определенного преобразования u_1', которое есть либо инверсия в E_1 степени >0, сфера которой ортогональна к C (упражнение 13), либо симметрия относительно некоторой гиперплоскости пространства E_1, проходящей через 0. (Рассмотреть в E_1 инверсию u_1 той же степени и с тем же полюсом, что u.) Сформулировать соответствующее предложение для симметрии v' в C, соответствующей некоторой симметрии v в L относительно гиперплоскости.

в) Рассмотрим на векторном пространстве $E_2 = A \times E_1$ квадратичную форму Q_2, определенную равенством

$$Q_2((\zeta, y))=\zeta^2-Q_1(y), \quad \zeta \in A, \quad y \in E_1;$$

эта форма невырождена, и сигнатура ее равна $(1, n+1)$. Отожде-

ствим E_1 с его каноническим образом в проективном пространстве $\boldsymbol{P}(E)_2$ (гл. II, приложение III, n° 4). Показать, что (в обозначениях б)) инверсия u' является также сужением на C некоторого проективного линейного отображения u'', получающегося путем факторизации из элемента u'' ортогональной группы $\boldsymbol{O}(Q_2)$, являющегося симметрией относительно неизотропной гиперплоскости в E_2. Сформулировать соответствующее предложение для v'. Вывести отсюда, что конформная группа пространства L изоморфна факторгруппе группы $\boldsymbol{O}(Q_2)$ по ее центру (использовать предложение 5 и упражнение 17в) § 6). Получить отсюда, что всякое преобразование из конформной группы есть произведение не более чем $n+2$ преобразований, каждое из которых есть либо инверсия, либо симметрия в L (см. § 6, упражнение 15д)).

г) Пусть Σ — множество, состоящее из сфер и гиперплоскостей аффинного пространства L. Вывести из б), что существует биекция множества Σ на дополнение в $\boldsymbol{P}(E_2)$ множества элементов $x \in E_1$ таких, что $Q_1(x) \leqslant 1$; отсюда следует, что точки, соответствующие двум ортогональным сферам, сопряжены относительно C.

15) Обобщить определения и результаты упражнений 12, 13 и 14 на случай, когда A — пифагорово поле и существует базис, ортонормальный относительно Ф.

16) Пусть A — поле, V — векторное пространство над полем A нечетной размерности $2r+1$, F — пространство $A \times V$, Ψ — невырожденная знакопеременная форма на F; множество C_0 прямых проективного пространства $\boldsymbol{P}(F)$ размерности $2r+1$, являющихся каноническими образами вполне изотропных плоскостей пространства F (относительно Ψ), называется (*проективным*) *линейным комплексом* в $\boldsymbol{P}(F)$, ассоциированным с формой Ψ.

В дальнейшем мы предполагаем, что A — максимальное упорядоченное поле; пусть Ф — невырожденная положительная симметрическая форма на V. Пусть D — прямая, ортогональная (относительно Ψ) к подпространству V в F, лежащая в V, и H — гиперплоскость в V, ортогональная к D (относительно Ф); в пространстве F H является неизотропным подпространством относительно Ψ, и его ортогональное подпространство (относительно Ψ) является, следовательно, плоскостью, дополняющей H и содержащей D. Множество C пересечений вполне изотропных (относительно Ψ) плоскостей пространства F, не содержащихся в V, с аффинным пространством $E = \{1\} \times V \subset F$ называется (*аффинным*) *линейным комплексом* в E, ассоциированным с формой Ψ; прямая $\Delta = P \cap E$ называется *осью* линейного комплекса C (для структуры евклидова пространства, определенного на E метрической формой Ф).

а) Показать, что в пространстве E всякий перенос, равный направляющему вектору прямой Δ (гл. II, приложение II, n° 3), оставляет комплекс C инвариантным (см. § 4, упражнение 6).

б) Пусть $(e_i)_{0\leqslant i\leqslant 2r}$ — ортонормальный базис пространства V относительно Φ, причем $e_0 \in D$ и $\Psi(e_{2i-1}, e_{2i}) = \varrho_i > 0$ для $1 \leqslant i \leqslant r$, $\Psi(e_j, e_k) = 0$ для пар индексов, не имеющих вида (e_{2i-1}, e_{2i}) или (e_{2i}, e_{2i-1}) (§ 7, n° 3, предложение 6). Выберем в аффинном пространстве E начало $a \in \Delta$ и положим $\Psi(a, e_0) = \varrho_0$. Пусть x — вектор из плоскости, порожденной векторами e_{2i-1} и e_{2i}, и y — вектор из этой же плоскости такой, что $\Phi(x, y) = 0$, $\Phi(y, y) = 1$, и $x \wedge y = \lambda e_{2i-1} \wedge e_{2i}$ для $\lambda > 0$. Пусть E_i — аффинное линейное многообразие размерности 3, порожденное точками a, $a + e_0$, $a + e_{2i-1}$, $a + e_{2i}$ в пространстве E, и R_x — пересечение E_1 с аффинной гиперплоскостью (в E), порожденной прямыми комплекса C, содержащими точку $a + x$. Показать, что направляющее подпространство прямых, ортогональных (относительно Φ) к плоскости R_x в многообразии E_i, есть прямая L_x, лежащая в плоскости $Ae_0 + Ay$, причем в случае, когда плоскость $Ae_0 + Ay$ ориентирована таким образом, что бивектор $e_0 \wedge y$ положителен, выполняется равенство

$$\operatorname{tg}\vartheta = \frac{\varrho_i}{\varrho_0}\sqrt{\Phi(x, x)},$$

где $\vartheta = \widehat{(D, L_x)}$.

*17) а) Пусть A — поле, $J\colon \xi \to \bar{\xi}$ — инволютивный автоморфизм поля A, E — векторное пространство размерности 2 над полем A, Φ — невырожденная (не знакопеременная) эрмитова полуторалинейная форма на пространстве E, (e_1, e_2) — ортогональный относительно Φ базис пространства E (§ 6, n° 1, теорема 1) такой, что

$$\Phi(\xi_1 e_1 + \xi_2 e_2,\ \eta_1 e_1 + \eta_2 e_2) = \alpha\xi_1\bar{\eta}_1 + \beta\xi_2\bar{\eta}_2$$

(α и β принадлежат полю K инвариантных элементов автоморфизма J); положим $\gamma = \beta/\alpha$. Отождествим точку $\xi_1 e_1 + \xi_2 e_2 \in E$ с элементом $\xi_1 + \xi_2\varrho$ кольца B, определенного условиями $\varrho^2 = -\gamma$, $\varrho\xi = \bar{\xi}\varrho$ для $\xi \in A$ (§ 3, упражнение 4а)). Для всякого $x = \xi_1 + \xi_2\varrho \in B$ положим $\tilde{x} = \bar{\xi}_1 - \xi_2\varrho$ и $N(x) = x\tilde{x} = \tilde{x}x$; тогда отображение $x \to \tilde{x}$ будет инволютивным антиавтоморфизмом алгебры B (над полем K) и $\Phi(x, x) = \alpha N(x)$. Показать, что всякое подобие относительно Φ, определитель которого равен коэффициенту подобия (называемое также *прямым* подобием), единственным образом может быть представлено в виде $x \to xy$, где y — неизотропный вектор пространства E, и коэффициент этого подобия равен $N(y)$.

б) Предположим сначала, что J — тождественный автоморфизм, так что $K = A$. Получить результаты n° 1 в случае, когда характеристика поля $A \neq 2$. Развить соответствующую теорию, когда характеристика поля A равна 2 (см. § 4, упражнение 14; разобрать два случая: γ является или нет квадратом в поле A).

в) Предположим, что $J \neq 1$, так что A — сепарабельное квадратичное расширение поля K; тогда Φ обязательно удовлетворяет

условию (Т) (§ 4, n° 2 и упражнение 1); если индекс формы Φ равен 0, то B — *рефлексивное* тело с центром K (гл. VIII, § 11, упражнение 4); если же индекс формы Φ равен 1, то B изоморфно $M_2(K)$.

г) Предположим, что $J \neq 1$ и характеристика поля $A \neq 2$; тогда $A = K(\vartheta)$ и $\vartheta^2 = -\delta \in K$; пусть S — группа прямых подобий относительно Φ, H — группа гомотетий в пространстве E с коэффициентом $\neq 0$, принадлежащим K (эта группа изоморфна K^*). Показать, что группа S/H изоморфна группе вращений $O^+(Q)$, где Q — невырожденная квадратичная форма на векторном пространстве F размерности 3 над полем K такая, что в F существует ортогональный базис (f_1, f_2, f_3), относительно которого

$$Q(\zeta_1 f_1 + \zeta_2 f_2 + \zeta_3 f_3) = \gamma\zeta_1^2 + \delta\zeta_2^2 + \gamma\zeta_3^2$$

(см. § 9, упражнение 15).

*18) Пусть A — поле, $\xi \to \bar{\xi}$ — инволютивный автоморфизм поля A, E — векторное пространство четной размерности $2m$ над полем A, Φ — невырожденная эрмитова форма индекса 0 на пространстве E, удовлетворяющая условию (Т), Δ — дискриминант формы Φ относительно некоторого базиса пространства E. Пусть $M(\Phi)$ — группа коэффициентов подобий относительно Φ (§ 4, упражнение 8). Показать, что $M(\Phi)$ есть подгруппа мультипликативной группы элементов кольца A, имеющих вид $\alpha\bar{\alpha} - (-1)^m \beta\bar{\beta}\Delta$. (Применить индукцию по m, используя упражнение 17 и следующие два замечания: 1° если u — подобие с коэффициентом μ, x — вектор пространства E, $y = u(x)$ и $z = u(y)$, то существует унитарное преобразование v такое, что $v(y) = y$ и $v(z) = \mu x$; 2° если α, β, λ — отличные от 0 элементы поля A такие, что существуют a, b, c, $d \in A$, удовлетворяющие условиям $\lambda = a\bar{a} + \alpha c\bar{c}$, $\lambda = b\bar{b} + \beta d\bar{d}$, то существуют s, t такие, что $\lambda = s\bar{s} - \alpha\beta t\bar{t}$.)

б) Пусть K — максимальное упорядоченное поле, $K_1 = K((t_1))$ — поле формальных степенных рядов от одного переменного t_1 с коэффициентами из поля K (гл. IV, § 5, n° 7), $A = K_1((t_2))$ — поле формальных степенных рядов от другого переменного t_2 с коэффициентами из K_1. Пусть E — векторное пространство размерности 6 над полем A, Q — невырожденная квадратичная форма на пространстве E, для которой существует ортогональный базис (e_i) такой, что

$$Q\left(\sum_{i=1}^{6} \xi_i e_i\right) = \xi_1^2 + \xi_2^2 + \xi_3^2 + \xi_4^2 + t_1\xi_5^2 + t_2\xi_6^2.$$

Показать, что не существует подобия относительно Q, коэффициент которого равен $t_1 t_2$.

ИСТОРИЧЕСКИЙ ОЧЕРК

К ГЛАВЕ IX

(Римские цифры относятся к библиографии в конце настоящего очерка.)

Теория квадратичных форм в ее современном виде восходит лишь ко второй половине XVIII в. и, как мы увидим, развивалась, прежде всего, в связи с запросами арифметики, анализа и механики. Однако основные понятия этой теории появились фактически вместе с «евклидовой геометрией» и составляют ее каркас. Поэтому нельзя проследить историю ее развития, не говоря, хотя бы вкратце, о развитии, начиная с античности, «элементарной геометрии». Разумеется, мы коснемся лишь нескольких самых общих идей, и читатель не должен надеяться найти здесь точные справки об истории той или иной отдельной теоремы; по этим вопросам следует обратиться к специальным трудам исторического и дидактического характера *). Разумеется также, что в случаях, когда мы ниже говорим о различных возможных интерпретациях одной и той же теоремы на различных алгебраических или геометрических языках, мы ни в коей мере не собираемся утверждать, что эти «переводы» во все времена были столь же хорошо известны, как сейчас; совсем наоборот, целью этого очерка и является показать, как математики постепенно, шаг за шагом, осознавали родство между этими вопросами, столь различными внешне; мы покажем также, как в процессе этого им удалось навести некоторый порядок в обилии геометрических теорем, оставленных древними, и попытаться, наконец, точно определить, что следует понимать под «геометрией».

Если оставить в стороне открытые вавилонянами формулы решения квадратного уравнения ((I), стр. 183—189), то зарождение главных понятий теории квадратичных форм нужно искать в геометрии. Прежде всего появляются квадраты расстояний (в плоскости и в трехмерном пространстве), и соответствующее понятие «ортогональности» вводится с помощью прямого угла, определенного Евклидом как половина развернутого угла (Начала, Книга I, определение 10); при этом понятия расстояния и угла

*) См. (II), а также E. Kötter, Die Entwickelung der synthetischen Geometrie, Leipzig (Teubner), 1901 (Jahresber. der Deutschen Math. Verein., т. V, 1. Heft) и Enzyklopädie der Math. Wiss., 1 ed., т. III.

связываются теоремой Пифагора, являющейся основой евклидовой геометрии *). Сама идея угла возникла, видимо, очень рано в греческой математике (и, несомненно, была заимствована греками у вавилонян, привыкших к ее использованию в своем богатом астрономическом опыте). Известно, что в классическую эпоху были определены лишь углы, меньшие двух прямых (впрочем, евклидово «определение» столь же расплывчато и практически неприменимо, как и определения, даваемые для прямой и плоскости); понятие ориентации выявлено не было, хотя Евклид и использует (без каких бы то ни было аксиом и определений) тот факт, что прямая разделяет плоскость на две области, которые он при необходимости заботливо различает **). Следовательно, к этому времени идея группы вращений в плоскости появляется лишь в очень несовершенном виде — с помощью сложения (введенного, снова без объяснения, Евклидом) неориентированных углов между полупрямыми, определенного в принципе лишь в случае, когда сумма не превосходит двух прямых углов ***). Что касается тригонометрии,

*) Большинство известных цивилизаций (Египет, Вавилония, Индия, Китай), по-видимому, независимо пришли к утверждениям, покрывающим по крайней мере некоторые частные случаи «теоремы Пифагора», а индусы имели даже идею доказательства этой теоремы, совершенно отличную от тех, что мы находим у Евклида (который дает два ее доказательства, одно — с построением вспомогательных фигур и другое, использующее теорию пропорций) (см. (II), т. IV, стр. 135—144).

**) Понятие ориентированного угла с различными его вариантами (угол между прямыми, угол между полупрямыми) появилось лишь гораздо позже. Эйлер ((VIIIa), стр. 217—239 и 305—307) вводит в аналитической геометрии полярные координаты и современную концепцию угла (измеряемого радианами), принимающего произвольные (положительные) значения. Л. Карно (Géométrie de Position, Paris, 1803) положил начало тенденции, в течение всего XIX в. противопоставлявшей «синтетическую» и аналитическую геометрии; пытаясь развить первую как можно более независимо, он, для того чтобы избежать «случаев расположения фигур» античной геометрии, вынужден систематически вводить ориентированные величины, углы и длины; к сожалению, его работа значительно усложнена стремлением не использовать отрицательные числа (которые он считал противоречивыми!), а заменять их малоудобной системой «соответствия знаков» между различными фигурами. Только Мебиус (XIII с) вводит концепцию ориентированного угла в рассуждении синтетической геометрии; однако Мебиус, как и его последователи вплоть до самого недавнего времени, может вводить ориентацию лишь прямым обращением к пространственной интуиции (правило «человечка Ампера»); лишь с развитием n-мерной геометрии и алгебраической топологии появилось, наконец, строгое определение «ориентированного угла».

***) В то же время мы находим у Евклида по меньшей мере два отрывка, где он говорит об углах, «сумма» которых превосходит два прямых, именно — при рассмотрении неравенств, которым должны удовлетворять плоские

то она не пользуется вниманием геометров и оставляется ими землемерам и астрономам; именно эти последние (Аристарх, Гиппарх и особенно Птолемей (V)) устанавливают фундаментальные соотношения между сторонами и углами прямоугольного треугольника (плоского и сферического) и составляют первые таблицы (имеются в виду таблицы, дающие *хорду* дуги, вырезаемой углом $\vartheta < \pi$ на окружности радиуса r, другими словами, число $2r \sin \frac{\vartheta}{2}$; введением синуса, более удобного в обращении, мы обязаны индийским математикам средних веков); при составлении этих таблиц неизвестиая в то время формула сложения дуг заменяется эквивалентным использованием теоремы Птолемея (восходящей, может быть, к Гиппарху) о четырехугольнике, вписанном в круг (см. Векторные топологические пространства, гл. V, § 1, упражнение 5). Следует также отметить, что Евклид и Герон указали предложения, эквивалентные формуле

$$a^2 = b^2 + c^2 - 2bc \cos A$$

для сторон и углов произвольного плоского треугольника; однако вряд ли стоит видеть здесь первое появление понятия билинейной формы, ассоциированной с метрической формой — ведь отсутствует еще идея векторного исчисления, возникшего лишь в XIX в.

Перемещения (и движения — различие между этими двумя понятиями не было ясно не только в античные времена, но и гораздо позднее) Евклиду были известны; однако по непонятным нам причинам он имел явно предубеждение против их использования (иапример, в теоремах о «случаях равенства треугольников», где создается впечатление, что он использует понятие перемещения исключительно потому, что не может сформулировать подходящую аксиому ((III bis), т. I, стр. 225—227 и 249)); тем не менее именно понятие перемещения (вращения вокруг оси) используется им для определения конусов вращения и сфер (Начала, Книга IX, определения 14 и 18), так же, как это делал Архимед для определения квадрик вращения. Но общая идея преобразования в применении ко всякому пространству в большой степени была чуждой для математической мысли вплоть до конца XVIII в. *); до XVIII в. мы не находим следов понятия композиции движений и тем более композиции перемещений. Это не означает, разумеется, что

углы трехгранного угла (Начала, Книга XI, предложения 20 и 21) (не говоря о «рассуждении» о «мере» углов, которое, несомненно, является вставкой (см. Исторический очерк к гл. VIII, Книга III); таким образом, в этих примерах, видимо, интуиция влечет Евклида гораздо дальше, чем позволяют его собственные определения. Его последователи были еще менее скрупулезны, и, например, Прокл (V в. до н. э.), не колеблясь, формулирует общую «теорему» о сумме углов выпуклого многоугольника ((III bis), т. I, стр. 322).

*) Как примеры этого понятия можно привести разве что «проекции» картографов и чертежников; стереографическая проекция (§ 10, упражнение 14) известна Птолемею (но лишь в XVIII в. стало известно, что она сохраняет углы), а центральная проекция играет первостепенную роль в ра-

греки не ощущали достаточно хорошо «регулярности» и «симметрии» геометрических фигур — свойства, которые мы связываем теперь с понятием группы перемещений; их теория правильных многоугольников и в еще большей степени теория правильных многогранников — одна из наиболее замечательных глав всей греческой математики — здесь же свидетельствуют об обратном *).

Наконец, последним существенным вкладом греческой математики в область, рассматриваемую нами здесь, является теория коник (что касается квадрик, то греки знали лишь некоторые квадрики вращения и, за исключением сферы, не продвинули их изучение достаточно далеко). Интересно отметить здесь, что хотя у греков никогда не было основной идеи аналитической геометрии (главным образом, из-за отсутствия подходящей алгебры), но мимоходом, при изучении «фигур» частного вида, они свободно использовали «координаты» относительно двух (и даже больше чем двух) осей в плоскости (эти оси близко связывались с фигурой, и это — главное, что отличает их метод от метода Ферма и Декарта, у которых оси фиксированы независимо от рассматриваемой фигуры). В частности, первые примеры коник (отличных от окружности), введенные в связи с задачей удвоения куба, представляли собой кривые, задаваемые уравнениями $y^2 = ax$, $y = bx^2$, $xy = c$ (Менехм, ученик Евдокса, середина IV в.) **); эти уравнения коник (отнесенные обычно к двум наклонным осям, образованным некоторым диаметром и касательной, проведенной в одной из точек его пересечения с кривой) чаще всего использовались при изучении задач, относящихся к самим этим кривым (тогда как «фокальные» свойства не играют большой роли, вопреки тому, как это можно подумать, судя по школьной традиции, которая восходит лишь к XIX в.). Из всей этой обширной теории мы остановимся здесь лишь на понятии сопряженных диаметров (известном уже Архимеду) и на свойстве, которое и в настоящее время служит для определения поляры

ботах Дезарга (VI); но при этом речь идет о соответствии между всем пространством (или поверхностью) и плоскостью. Одно из свойств инверсии, свойство, которое мы теперь выражаем словами, что инверсия переводит окружность в окружность или в прямую (см. § 10, упражнение 13), известно, по существу, Виета и используется им в задачах на построение окружностей; но ни он, ни Ферма, распространивший его построения на сферы, не имели в виду введения инверсии как некоторого преобразования плоскости или пространства.

*) См. выше, A. S p e i s e r, Theorie der Gruppen von endlicher Ordnung, Basel (Birkhäuser, 4 édit., 1956), где можно также найти интересные замечания о связи между теорией групп перемещений и различными типами орнаментов, созданных античной и средневековой цивилизациями.

**) По-видимому, идея рассмотрения этих кривых как сечений плоскостью конуса с круговым основанием (принадлежащая также Менехму) возникла уже *после* их определения с помощью указанных уравнений (см. (IV), стр. XVII — XXX).

точки, данном Аполлонием (IV) для случая, когда точка лежит вне конпки (и, следовательно, ее полярой является прямая, соединяющая точки касания двух касательных, проведенных из данной точки); с нашей точки зрения, эти понятия представляют собой первые два примера «ортогональности» относительно квадратичной формы, отличной от метрической, но, само собой разумеется, их связь с классическим понятием перпендикуляра в то время никак не могла быть осознана.

До Декарта и Ферма нельзя указать каких-либо новых достижений в этой области; однако уже с самого начала аналитической геометрии алгебраическая теория квадратичных форм начинает сбрасывать геометрическую оболочку; Ферма уже знает, что уравнение второй степени изображает в плоскости некоторую конику ((VIIa), стр. 100—102), и набрасывает аналогичные идеи для квадрик (VII b). В течение XVIII в. с развитием аналитической геометрии двух и трех измерений поля возникают (особенно в связи с кониками и квадриками) две центральные задачи этой теории: приведение квадратичной формы к сумме квадратов и разыскание ее «осей» относительно метрической формы. Для коник обе эти задачи слишком элементарны, для того чтобы привести к существенному алгебраическому прогрессу; первая из них для произвольного числа переменных решена Лагранжем в 1759 г. в связи с нахождением максимума функций многих переменных (IXa). Однако эта проблема почти сразу же была отодвинута на второй план задачей нахождения осей, даже до того, как была сформулирована инвариантность ранга *); что касается закона инерции, то он был открыт лишь около 1850 г. Якоби (XIX b), доказавшим его тем же способом, что используется в настоящее время, и Сильвестром (XX), который ограничился его формулировкой как почти очевидного предложения **).

Задача приведения квадрики к ее осям представляла алгебраические трудности, уже заметно большие, чем аналогичная задача для коник. Эйлер, первый приступивший к ней, оказался не в состоянии доказать действительность собственных значений и принял это после некоторого наброска обосно-

---

*) Исследуя одну проблему, не зависящую по своей природе от выбора осей координат, Лагранж не мог не заметить, что его метод оставляет много возможностей для произвола; но ему не хватает понятий, чтобы уточнить эту идею: «*Впрочем*, — пишет он,— *для того чтобы в этих исследованиях не ошибиться, необходимо отметить, что преобразованные* [к сумме квадратов] *формы могут оказаться отличными от тех, что мы задали; однако, проверяя это ближе, мы неизменно убеждаемся, что, каковы бы они ни были, они всегда могут быть сведены к исходным или по крайней мере в них содержатся*» [?] ((IX), стр. 8).

**) Гаусс, со своей стороны, пришел к этому результату и, по свидетельству Римана, слушавшего его лекции в 1846—1847 гг., доказывал его на этих лекциях методом наименьших квадратов (B. Riemann, Gesammelte Werke, Nachträge, Leipzig (Teubner), 1902, стр. 59).

вания, не имевшего доказательной силы ((VIIIa), стр. 379—392) *). Хотя к 1800 г. это утверждение было корректно установлено, лишь Коши доказал его для произвольного числа n переменных (XIVb). В это же время Коши доказывает, что характеристическое уравнение, дающее собственные значения, инвариантно при любом изменении прямоугольных осей ((XIVa), стр. 252 **)); при $n = 2$ и $n = 3$ эта инвариантность интуитивно «очевидна» из соображений геометрической интерпретации собственных значений с помощью осей соответствующей коники или квадрики. Кроме того, в ходе этих исследований естественным образом появились элементарные симметрические функции от собственных значений (в различных геометрических интерпретациях и особенно в связи с теоремами Аполлония о сопряженных диаметрах), в частности дискриминант (давно уже известный для $n = 2$ в связи с теорией квадратных уравнений), впервые появившийся при $n = 3$, видимо, у Эйлера ((VIIIa), стр. 382); Эйлер находит его при классификации квадрик (выражая условие того, что квадрика не имеет бесконечно удаленной точки) и не отмечает его инвариантности при изменении прямоугольных осей. Но несколько позже, с появлением арифметической теории квадратичных форм, Лагранж замечает (при $n = 2$) один частный случай инвариантности дискриминанта при линейном, но не ортогональном преобразовании переменных ((IXb), стр. 699), а Гаусс устанавливает для $n = 3$ «ковариантность» дискриминанта относительно любого линейного преобразования ((XIa), стр. 301—302) ***). Как только Коши и Бине доказали общую формулу для произведения определителей, формула Гаусса была немедленно распространена на случай произвольного числа переменных; именно эта формула в 1845 г. дала первый толчок к общей теории инвариантов.

К двум понятиям, которыми греки заменяли теорию перемещений,— к понятиям движения и «симметрии» геометрической фигуры — к XVII—XVIII вв. прибавляется третье — изменение прямоугольных осей, эквивалентное, по существу, теории перемещений. Этому вопросу Эйлер посвя-

---

*) Более удачно у Эйлера получилось нахождение главных осей инерции твердого тела: сведя задачу к уравнению третьей степени, он заметил, что такое уравнение имеет по крайней мере один действительный корень, и следовательно, имеется по крайней мере одна ось инерции; взяв эту ось в качестве оси координат, он сводит задачу к легко решаемой плоской задаче ((VIIIb), стр. 200—202).

**) Надо отметить, что вплоть до 1930 г. под «квадратичной формой» понимали однородный многочлен второй степени от координат, взятых в некоторой данной системе осей. Видимо, лишь теория гильбертовых пространств привела к «внутренней» концепции квадратичных форм даже в пространствах конечной размерности.

***) Также в связи с этими исследованиями Гаусс определил обратную форму для квадратичной формы ((XIa), стр. 301) и получил условие ее положительности (§ 7, n° 1, предложение 3), в котором используются главные миноры определителя (там же, стр. 305—307).

щает несколько работ, стремясь, прежде всего, получить удобное параметрическое представление для формул перемены осей. Известно, какую пользу принесли механике три угла, введенные им для этой цели ((VIIIa), стр. 371—378). Не ограничившись этим, в 1770 г. он рассматривает общую проблему ортогональных преобразований для произвольного n, замечает, что в этом случае к цели приводит введение $n(n-1)/2$ углов как параметров, и, наконец, для $n=3$ и $n=4$ указывает *рациональные* представления вращений (как функции соответственно 4 и 8 однородных параметров, связанных некоторым соотношением), которые позже были получены с помощью теории кватернионов (см. § 9, упражнения 15 и 16); о происхождении этих формул Эйлер ничего не говорит (VIIIc) *). С другой стороны, Эйлер указывает, как переводится на аналитический язык отысканне «симметрии» плоской фигуры, и именно в связи с этим приходит к доказательству, по существу, того, что всякое перемещение плоскости является вращением, или переносом, или переносом с последующей симметрией ((VIIIa), стр. 197—199). Быстрое развитие механики в эту эпоху привело к общему изучению перемещений; однако вначале рассматривались лишь «бесконечно малые» перемещения, направленные по касательной к непрерывным движениям: только они встречаются в исследованиях Торичелли, Роберваля и Декарта о композиции движений и мгновенном центре вращения движения в плоскости (см. Исторический очерк к книге IV, гл. I, II, III). Мгновенный центр вращения в общем виде был найден Иоганном Бернулли; в 1749 г. Даламбер, а годом позже Эйлер расширили это понятие, доказав существование мгновенной оси вращения для движений, оставляющих неподвижной некоторую точку. Аналогичная теорема для конечных перемещений сформулирована лишь в 1775 г. Эйлером (VIIId) в мемуаре, где он обнаружил вместе с тем, что определитель вращения равен 1; в следующем году он доказывает существование неподвижной точки для любого подобия в плоскости (VIIIe). Однако лишь в работах Шаля, начиная с 1830 г. (XVa), оформилась, наконец, стройная теория конечных и бесконечно малых перемещений.

* * *

Итак, мы подошли к периоду, который называют золотым веком геометрии и который длится grosso modo от публикации «Описательной геометрии» Монжа (1795) (X) и до «Эрлангенской программы» Клейна (1872) (XXV b). Основные достижения, которыми мы обязаны этому внезапному возрождению геометрии, состоят в следующем:

---

*) Впрочем, Эйлер не дает формулы для композиции вращений, выраженной с помощью этих параметров; для $n=3$ эта формула не была известна до заметки Гаусса (не опубликованной при его жизни (XIb)) и одной работы Олинда Родригеса (1840 г.), который вновь приходит к параметрическому представлению, полученному Эйлером и находившемуся в то время в почти полном забвении.

А) Понятие бесконечно удаленного элемента (точки, прямой или плоскости), введенное Дезаргом в XVII в. (VI), но вплоть до XVIII в. считавшееся лишь некоторой вольностью речи, было реабилитировано и систематически использовалось Понселе (XII), заключившим тем самым проективную геометрию в общие рамки для всех геометрических явлений.

Б) В то же самое время Монж и в особенности Понселе совершили переход к *комплексной* геометрии. С помощью понятия мнимой точки, спорадически возникавшего в течение XVIII в. (а также понятия бесконечно удаленной точки), они дают формулировки, не зависящие от «случаев расположения фигур» в действительной аффинной геометрии. Хотя в самом начале обоснования этих нововведений встречали сильнейшее сопротивление (особенно со стороны школы «синтетической» геометрии, в которой применение координат считалось позором), здесь в «принципе возможных случайных отношений» Монжа или в «принципе непрерывности» Понселе нельзя не распознать первого ростка идеи «специализации» из современной алгебраической геометрии *).

Одним из первых результатов, полученных на основе этих концепций, было замечание, что в комплексном проективном пространстве все невырожденные коники (соответственно квадрики) имеют одну и ту же природу; это утверждение привело Понселе к открытию «изотропных» элементов: «*Окружности, расположенные произвольным образом*,— пишет он,— *не являются, следовательно, совершенно независимыми друг от друга, как можно подумать с первого взгляда, и идеально имеют общую мнимую точку в бесконечности*» ((XII), стр. 48). Далее он вводит аналогичным образом «омбилическую кривую», мнимую бесконечно удаленную конику, общую для всех сфер ((XII), стр. 370); и если он не говорит особо об изотропных образующих сферы, то по крайней мере явно подчеркивает существование прямолинейных образующих, мнимых или действительных, у всех квадрик (там же, стр. 371) **); последователи Понселе (особенно Плюкер и Шаль) еще в большей степени, чем он сам, используют эти понятия, в частности, при изучении «фокальных» свойств коник и квадрик.

В) Понятия *точечного преобразования* и композиции преобразований были сформулированы в общем виде и систематически использовались в процессе доказательств. К тому времени, кроме перемещений и проекций, были известны лишь отдельные частные преобразования: некоторые проективные

---

*) Эти «принципы» обосновываются, естественно (как это заметил уже Коши), применением принципа продолжения алгебраических тождеств, ибо «синтетические» геометры рассматривают лишь такие свойства, которые переводятся на аналитический язык тождествами такого рода.

**) Впервые прямолинейные образующие квадрик были, по-видимому, замечены Реном (1669 г.), который обнаружил, что однополостный гиперболоид вращения может быть получен вращением некоторой прямой вокруг оси, не лежащей с ней в одной плоскости; но изучение их было развито лишь Монжем и его школой.

преобразования типа $x' = a/x$, $y' = y/x$, применявшиеся Лагиром и Ньютоном, «аффинное преобразование» $x' = ax$, $y' = by$ Клеро и Эйлера и, наконец, несколько частных квадратичных преобразований у того же Ньютона, Маклорена и Брекенриджа. В своей «Описательной геометрии» Монж демонстрирует всю пользу, которую можно извлечь из плоских проекций в геометрии трех измерений. Одним из методом, систематически и даже сверх меры применявшимся Понселе в доказательствах, было сведение с помощью проекции свойств коники к свойствам окружности (этот метод уже употребляли при случае Дезарг и Паскаль); и для того чтобы проделать аналогичное сведение квадрики к сфере, Понселе изобретает первый пример проективного преобразования пространства —«гомологию» ((XII), стр. 357); наконец, именно им введены первые примеры бирациональных преобразований некоторой кривой на себя. В 1827 г. Мебиус ((XIIIa), стр. 217) (и независимо от него в 1830 г. Шаль (XV b)) определяет проективное преобразование самого общего вида; в это же время появляется инверсия (см. § 10, упражнение 13) и другие типы квадратичных преобразований, изучение которых положило начало теории бирациональных преобразований, получившей свое развитие во второй половине XIX в.

Г) Понятие *двойственности* появляется сразу с полной ясностью и сознательно связывается с теорией билинейных форм. Теория полюсов и поляр относительно коник, которая со времен Аполлония проделала некоторое развитие лишь благодаря Декарту и Лагиру, обобщается на квадрики Монжем, который, так же как его ученики, замечает возможность с помощью этой теории известные теоремы переформулировать как новые результаты *). И снова Понселе принадлежит здесь честь превращения этих отдельных замечаний в общий метод созданной им теории преобразований «посредством взаимных поляр», оказавшийся чрезвычайно эффективным. Немного позже, в основном у Жергона, Плюкера, Мебиуса и Шаля, общее понятие двойственности освобождается от связи с квадратичными формами, еще слишком близкой у Понселе. В частности, Мебиус, рассматривая различные варианты двойственности в трехмерном пространстве (определенной билинейной формой), обнаруживает в 1833 г. двойственность относительно знакопеременной формы (XIII b)**), которая в XIX в. интенсивно изучалась как теория «линейных комплексов» (см. § 10, упражнение 16) и развивалась в связи с «геометрией прямых» и «плюкеровых координат», введенных около 1860 г. Кэли, Грассманом и Плюкером.

Д) Уже в самом начале развития проективной геометрии интенсивное изучение классических геометрических свойств в их связи с проективным пространством быстро привело к разделению этих свойств на «метрические»

*) Наиболее известна теорема Брианшона (1810 г.), получающаяся с помощью двойственности из теоремы Паскаля.

**) В 1828 г. Джорджини уже столкнулся с полярностью относительно знакопеременной формы в связи с одной проблемой статики (Mem. Soc. Ital. Modena, т. XX (1828), стр. 243—254).

и «проективные», и в этом, несомненно, без всякого преувеличения можно видеть очень четкое для того времени проявление того, что в дальнейшем превратилось в современное понятие структуры. Однако Понселе, который первый обнаружил это различие и ввел эту терминологию, осознавал уже и связь между этими двумя типами свойств и, приступая в своем «Трактате» к проблемам, относящимся к углам, писал, что их свойства «*не являются, по-видимому, теми, которые мы называем проективными..., но тем не менее столь просто вытекают из основных принципов* [этого труда]..., *что я не думаю, что какая-либо другая геометрическая теория могла бы привести к этому одновременно более непосредственно и более просто. И в этом нет ничего удивительного, если учесть, что проективные свойства фигур определенно являются наиболее общими из свойств, которыми могут обладать эти фигуры, а поэтому они должны содержать в себе в качестве простых следствий все остальные частные свойства или отношения в пространстве*» ((XII), стр. 248). Собственно говоря, после этой декларации несколько странно видеть, как он исследует свойства углов чрезвычайно искусственным способом, связывая их с фокальными свойствами коник, вместе того чтобы прямо использовать циклические точки; и в действительности лишь через 30 лет Лагерр (еще будучи учеником Политехнической школы) указал выражение угла между прямыми с помощью двойного отношения этих прямых и изотропных прямых, исходящих из этой точки (см. § 10, упражнение 5) ((XXI), т. I, стр. 13). Наконец, Кэли совсем ясно (XVIIId) формулирует фундаментальную мысль о том, что «метрические» свойства плоской фигуры являются «проективными» свойствами этой фигуры, дополненной циклическими точками, — решающий шаг на пути к «Эрлангенской программе».

Е) *Гиперболическая неевклидова геометрия*, возникшая около 1830 г., оставалась первое время несколько в стороне от того движения, основные линии которого мы здесь прослеживаем. Будучи результатом сомнений чисто логического порядка, касающихся оснований классической геометрии, эта новая геометрия была изложена ее создателями *) в той же «синтетической» и аксиоматической форме, что и геометрия Евклида, и без всякой связи с проективной геометрией (введение которой, согласно классической модели, казалось a priori исключенным, так как в этой геометрии нет единственной параллельной прямой); и несомненно, что именно поэтому она долгое время не привлекала внимания французской, английской и немецкой школ проективной геометрии. Поэтому, когда Кэли в цитированном выше

*) Известно, что Гаусс, начиная с 1800 г., был убежден в невозможности доказательства V постулата Евклида и в логической возможности развивать геометрию, в которой этот постулат неверен. Однако он не опубликовал эти результаты, и они были независимо найдены Лобачевским в 1829 г. и Бойаи в 1832 г. Детали можно найти в книге: F. Engel — P. Stäckel, Die Theorie der Parallellinien von Euklid bis auf Gauss, Leipzig (Teubner), 1895 и Urkunden zur Geschichte der nichteuklidischen Geometrien, т. 2, Leipzig (Teubner), 1898—1913.

основополагающем мемуаре (XVIIId) предлагает заменить циклические точки (рассматриваемые как «касательно вырожденные» коники) некоторой произвольной коникой (которую он называет «абсолютом»), он и не думает о том, чтобы связать эту идею с геометрией Лобачевского — Бойаи, хотя и указывает, как она приводит к новым выражениям для «расстояния» между двумя точками, и отмечает ее связь со сферической геометрией. Ситуация изменилась к 1870 г., когда благодаря трудам Лобачевского, опубликованию работ Гаусса и вступительной лекции Римана неевклидовы геометрии вышли на первый план в математике того времени. Следуя по пути, очерченному Риманом, Бельтрами, незнакомый с работой Кэли, вновь находит в 1868 г. полученные Кэли выражения для расстояния, но в совершенно другом контексте — при рассмотрении внутренней части круга как образа некоторой поверхности постоянной кривизны, геодезические линии которой являются прямыми (XXIV); двумя годами позже Клейн (независимо от Бельтрами) объединил эти две различные точки зрения и дополнил их открытием эллиптического неевклидова пространства (XXVa) *).

Ж) Вторая половина рассматриваемого здесь периода стала временем критических размышлений, в ходе которых сторонники «синтетической» геометрии, не удовлетворившись изгнанием координат из всех своих доказательств, настаивали на том, чтобы вообще обходиться без действительных чисел, в том числе и в геометрических аксиомах. Главным представителем этой школы был фон Штаудт, которому, по существу, удалось справиться с этим трудным делом (XXIII) и вызвать общее восхищение не только в свое время, но и в начале XX в.; и хотя в настоящее время мы не считаем подобные идеи заслуживающими внимания, поскольку возможности их плодотворного применения оказались слишком незначительными, но следует тем не менее отметить, что усилия фон Штаудта и его последователей содействовали уяснению роли действительных и комплексных «скаляров» в классической геометрии и созданию с их помощью современной концепции геометрии над произвольным основным телом.

К 1860 г. «синтетическая» геометрия достигла своей высшей точки, но конец ее господства приближался быстрыми шагами. Оставаясь на протяжении всего XVIII в. громоздкой и неуклюжей, аналитическая геометрия в руках Ламе, Бобилье, Коши, Плюкера и Мебиуса приобрела, наконец, краткость и изящество, которые дали ей возможность сразиться на равных со своей соперницей. Начиная примерно с 1850 г. понятия группы и инварианта, сформулированные, наконец, точным образом, постепенно завоевывают сцену, и все замечают, что теоремы классической геометрии являются лишь выражением тождественных соотношений между инвариантами или

*) Пример сферической геометрии некоторое время заставлял верить, что в пространстве постоянной положительной кривизны всегда существует пара точек, через которую проходит более одной геодезической.

ковариантами группы подобий *), а теоремы проективной геометрии в свою очередь выражают тождества (или «сизигии») между ковариантами проективной группы. Эта мысль была в совершенном виде изложена Клейном в знаменитой «Эрлангенской программе» (XXV b), где он призывает прекратить бесполезный спор между «аналитической» и «синтетической» тенденциями; если,— пишет он,— обвинение последней в том, что она ставит в привилегированное положение какую-то одну систему произвольных осей, «*слишком часто оправдывалось при том несовершенном способе использования координат, который когда-то ею употреблялся, то оно немедленно снимается, когда речь идет о рациональном применении этого метода... Область пространственной интуиции не закрыта для аналитического метода...*» и подчеркивает, что «*нельзя недооценивать преимуществ, которые приносит удачно приспособленный формализм в дальнейших исследованиях, где он, если можно так выразиться, опережает нашу мысль*» ((XXV b), стр. 488—490).

Тем самым была создана рациональная и «структурная» классификация теорем «геометрии» в соответствии с группой, которой они подчиняются: это линейная группа для проективной геометрии, ортогональная группа для метрических вопросов, симплектическая группа для геометрии «линейного комплекса». Однако в этом беспощадном свете классическая геометрия — за исключением алгебраической и дифференциальной геометрий **), уже представляющих собой отдельные дисциплины,— быстро увядает и теряет весь свой блеск. Уже обобщение методов, основанных на использовании преобразований, сделало несколько механическим получение новых теорем: «*В настоящее время*,— пишет Шаль в 1837 г. в своем «Историческом обзоре»,— *каждый может взять какую-нибудь известную истину и применять к ней различные общие принципы преобразований; так он получит новые истины, отличные от первоначальной или более общие; а эти истины также можно подвергнуть той же операции; таким образом, можно умножать чуть ли не до бесконечности число новых истин, полученных из первой... Следовательно, обобщать и создавать в геометрии при современном состоянии этой*

---

*) Например, первые члены уравнений трех высот треугольника являются ковариантами его трех вершин относительно группы подобий, и теорема, утверждающая, что эти три высоты пересекаются в одной точке, равносильна утверждению, что эти три ковариантa линейно зависимы.

**) Нет надобности излагать здесь историю этих двух дисциплин и детально исследовать влияние на их дальнейшее развитие «Эрлангенской программы». Отметим только, что алгебраическая геометрия после более чем столетнего развития стала изучаться интенсивно, как никогда раньше; что же касается дифференциальной геометрии, то после блестящего расцвета, который она познала в трудах Ли, Дарбу и их последователей, она находилась под угрозой оказаться в том же положении, что и элементарная геометрия, пока современные работы (проистекающие в особенности от идей Э. Картана) о расслоенных пространствах и «глобальных» проблемах не доказали ее жизнеспособности.

науки может каждый, кто этого захочет; для добавления камней к ее зданию гений больше не нужен» ((XV b), стр. 268—269). Еще более определенной становится ситуация в связи с успехами теории инвариантов, которая, наконец (по крайней мере для «классических» групп), выработала общие методы, позволяющие, в принципе, чисто автоматически описывать все алгебраические коварианты и все их «сизигии»; эта победа означала гибель как самостоятельного поля исследований сразу двух теорий: самой классической теории инвариантов и «элементарной» геометрии, ставшей практически простым словарем для теории инвариантов. Разумеется, нет никакой возможности предугадать a priori, какие из «бесконечного числа» теорем, которые можно таким образом при желании получить, можно сформулировать на геометрическом языке столь же просто и изящно, как и классические результаты, и здесь остается еще некоторая область, в которой с успехом применяют свои силы многочисленные любители (геометрия треугольника, тетраэдра, алгебраических кривых и поверхностей маленьких степеней и т. д.). Но с точки зрения математика профессионала, эта жила уже истощена, поскольку в ней нет больше проблем структуры, способных повлиять на другие разделы математики; и эта глава теории групп и инвариантов может считаться закрытой — до появления новых идей *).

* * *

Таким образом, после появления «Эрлангенской программы» евклидовы и неевклидовы геометрии с точки зрения чисто алгебраической стали просто-напросто языками, более или менее удобными для выражения результатов теории билинейных форм, успешно развивавшейся наравне с теорией инвариантов **). Все, что касается понятия ранга билинейной формы и связи между этими формами и линейными преобразованиями, было окончательно выяснено работами Фробениуса (XXVIIa). Ему же принадлежит каноническое выражение для билинейной формы над свободным $\boldsymbol{Z}$-модулем (§ 5, n° 1, теорема 1) (XXVII b); однако кососимметрические определители появляются впервые в начале века у Пфаффа в связи с приведением дифференциальных форм к нормальному виду. Якоби, который в 1827 г. возвращается к этой

*) Разумеется, это неизбежное падение геометрии (евклидовой и проективной), для нас совершенно очевидное, долгое время не замечалось современниками, и вплоть до 1900 г. ее продолжали считать одной из важных ветвей математики, о чем свидетельствует, например, место, которое она занимает в Enzyklopädie, и такое же самое место она занимала до сих пор в университетском преподавании.

**) В частности, интерес к неевклидовой геометрии проистекает не от этого банального алгебраического аспекта, но из-за ее связей с дифференциальной геометрией и теорией функций комплексного переменного; именно поэтому элементарные понятия и определения неевклидовой геометрии вводятся в этом трактате только в тех главах, где рассматриваются эти теории.

проблеме (XIXa), уже известно, что кососимметрический определитель нечетного порядка равен нулю; Якоби образует также выражение для пфаффиана и показывает, что он является делителем кососимметрического определителя четного порядка, но не замечает, что этот определитель является квадратом пфаффиана, что было установлено лишь Кэли в 1849 г. (XVIIIb). Понятие симметрической билинейной формы, ассоциированной с квадратичной формой, является самым элементарным случаем процесса «полярпзации», одного из основных рабочих инструментов теории инвариантов. Под именем «скалярного произведения» это понятие имело успех сначала среди популяризаторов «векторного исчисления», а с начала XXв.— благодаря неожиданным обобщениям, к которым оно привело в теории гильбертовых пространств (см. Исторический очерк к гл. V). Эта последняя теория вызвала также к жизни понятие сопряженного оператора (который до этого достаточно явно применялся лишь в теории линейных дифференциальных уравнений и в тензорном исчислении в вальсе ко- и контрвариантных индексов, послушных дирижерской палочке метрического тензора); наконец, именно эта теория выпукло подчеркнула понятие эрмитовой формы, введенное Эрмитом в 1853 г. в связи с его арифметическими исследованиями ((XXII), стр. 237), но вплоть до 1925 г. остававшееся вне поля зрения основных направлений математики, когда комплексные гильбертовы пространства были применены к квантовым теориям. С другой стороны, все большее и большее значение приобретает изучение ортогональной группы и группы подобий, явно выделенных и исследуемых с середины XIX в., ставших стержнем теории квадратичных форм, наравне с другими «классическими» группами (линейная группа, симплектическая группа и унитарная группа). Мы отметим здесь лишь существенную роль, которую играют эти группы в теории групп Ли и в дифференциальной геометрии, с одной стороны, и в арифметической теории квадратичных форм (см., например, (XXXIII) и (XXXV), с другой *); этим обстоятельством, равно как и распространением концепции двойственности на самые различные вопросы, объясняется тот факт, что нет ни одной современной математической теории, в которой тем или иным образом не использовались бы билинейные формы. Во всяком случае, мы должны отметить, что именно изучение группы вращения (трехмерного пространства) привело Гамильтона к открытию кватернионов (XVII); это открытие было обобщено В. Клиффордом, который в 1876 г. ввел в рассмотрение алгебры, носящие его имя, и доказал, что они являются тензорными произведениями алгебр кватернионов, или алгебр кватернионов и некоторого квадратичного расширения (XXVIII). Эти алгебры, найденные через четыре года Липшицем (XXIX), применявшим их для задания параметрического представления ортогонального преобразования n переменных (что

*) Не говоря уже о квантовых теориях, где широко используются линейные представления ортогональных групп, и о теории относительности, которая привлекла внимание к «группе Лоренца» (ортогональная группа относительно некоторой формы с сигнатурой (3,1)).

обобщало результаты, полученные Кэли для $n = 3$ (XVIIIa) и $n = 4$ (XVIIIc) с помощью теории кватернионов (см. § 9, упражнения 15 и 16)), эти алгебры, вместе с понятием «спинора», полученным из них Липшицем (см. (XXXII) и (XXXIV)), также должны были стать популярными в наше время в связи с их использованием в квантовых теориях.

Нам остается лишь сказать несколько слов об эволюции идей, которая привела к почти полному снятию ограничений на кольцо скаляров в теории полуторалинейных форм, — тенденция, общая для всей современной алгебры, но проявляющаяся здесь сильнее, чем в любом другом ее разделе. Мы уже отмечали плодотворность введения комплексной геометрии над полем комплексных чисел (которое, впрочем, в течение всего XIX в. проходило с постоянными и иногда опасными конфликтами между этой и действительной геометрией); ясность этой теории достигается в основном благодаря аксиоматическим исследованиям оснований геометрии в конце XIX в. В ходе этих исследований Гильберт и особенно его соперники, исследуя соотношения между различными аксиомами, пришли к построению соответствующих контрпримеров, в которых «основное тело» (коммутативное или нет) обладало более или менее патологическими свойствами, и тем самым приучили математиков к «геометриям» совершенно нового типа. С точки зрения аналитической уже Галуа рассмотрел линейные преобразования, коэффициенты которых принимают значения в некотором простом конечном поле ((XVI), стр. 27); развивая эти идеи, Жордан (XXVI) естественным образом пришел к рассмотрению классических групп над этими полями, групп, постоянно встречающихся в самых различных областях математики. В 1900 г. Диксон распространил результаты Жордана на произвольные конечные поля, а впоследствии было замечено, что большая часть теории Жордана — Диксона распространяется на случай, когда «основное тело» совершенно произвольно; это объясняется, в первую очередь, общими свойствами изотропных векторов и теоремой Витта, которые, будучи тривиальны в классических случаях, для произвольного «основного тела» установлены лишь в 1936 г. (XXXI) *).

Но при таком, все более и более «абстрактном» направлении развития теории полуторалинейных форм оставалось весьма желательным сохранить такую терминологию, которая в случае пространств 2 и 3 измерений проистекала бы из классической геометрии, и распространить ее на n-мерные и даже бесконечномерные пространства. Тем самым классическая геометрия, законченная как живая самостоятельная наука, превратилась в универсальный язык современной математики, чрезвычайно удобный и гибкий.

*) Более подробно об этих вопросах см. J. Dieudonné, La géométrie des groupes classiques (Erg. der Math., Neue Folge, Heft 5, Berlin — Göttingen — Heidelberg (Springer), 1955).

БИБЛИОГРАФИЯ

(I) O. Neugebauer, Vorlesungen über Geschichte der antiken mathematischen Wissenschaften, Bd. I: Vorgriechische Mathematik, Berlin (Springer), 1934.

(II) J. Tropfke, Geschichte der Elementar-Mathematik, т. IV—VI, Berlin — Leipzig (de Gruyter), 1923—1924.

(III) Euclidis Elementa, т. 5; éd. J. L. Heiberg, Lipsiae (Teubner), 1883—1888.

(III bis) T. L. Heath, The thirteen books of Euclid's Elements..., т. 3, Cambridge, 1908.

(IV) T. L. Heath, Apollonius of Perga, Treatise on conic sections, Cambridge (Univ. Press), 1896.

(V) Ptolemaei Cl. Opera, éd. J. L. Heiberg, т. 2, Lipsiae (Teubner), 1898—1903.

(VI) G. Desargues, Œuvres..., т. I, Paris (Leiber), 1864: Brouillon proiect d'nne atteinte anx événements des rencontres d'un cône avec un plan, стр. 103—230.

(VII) P. Fermat, Œuvres, т. I, Paris (Gauthier-Villars), 1891: a) Ad locos planos et solidos Isagoge, стр. 91—110 (франц., ibid., т. III, стр. 84—101); b) Isagoge ad locos ad superficiem, стр. 111—117 (франц., ibid., т. III, стр. 102—108).

(VIII) L. Euler: a) Introductio in Analysin Infinitorum (Opera Omnia (1), т. IX, Zürich — Leipzig — Berlin (O. Füssli et B. G. Teubner), 1945); b) Theoria motus corporum solidorum seu rigidorum (Opera Omnia (2), т. III, Zürich — Leipzig — Berlin (O. Füssli et B. G. Teubner, 1948); c) Problema algebraicum ob affectionus prorsus singularis memorabile (Opera Omnia (1), т. VI, Leipzig — Berlin (Teubner), стр. 287—315, 1921); d) Formulae generales pro translatione quacunque corporum rigidorum, Novi Comm. Acad. Sc. imp. Petrop., т. XX, стр. 189—207 (1776); e) De centro similitudinis (Opera Omnia (1), т. XXVI, Zürich (O. Füssli), стр. 276—285 (1956)).

(IX) J. L. Lagrange, Œuvres, Paris (Gauthier-Villars), 1867—1892: a) Recherches sur la méthode de maximis et minimis, т. I, стр. 3—20; b) Recherches d'arithmétique, т. III, стр. 695—795.

(X) G. Monge, Géométrie descriptive, Paris, 1798.

(XI) C. F. Gauss, Werke: a) Disquisitiones arithmeticae, т. I, Göttingen. 1870; b) Mutationen des Raumes, т. VIII, Göttingen. 1900. стр. 357—362.

(XII) J.-V. Poncelet, Traité des propriétés projectives des figures. т. I, 2 éd., Paris (Gauthier-Villars), 1865.

(XIII) A. F. Möbius, Gesammelte Werke, Leipzig (Hirzel), 1885—1887: a) Der barycentrische Calcul, т. I, стр. 1—388; b) Ueber eine besondere Art dualer Verhältnisse zwischen Figuren im Raume, т. I, стр. 489—515 (=J. de Crelle X (1833)); c) Ueber eine neue Behandlungsweise der analytischen Sphärik, т. II, стр. 1—54.

(XIV) A.-L. Cauchy: a) Leçon sur les application du calcul infinitésimal à la géométrie (Œuvres complètes (2), т. V, Paris (Gauthier-Villars), 1903); b) Sur l'équation à l'aide de laquelle on détermine les inégalités séculaires des planètes (Œuvres complètes (2), т. IX, Paris (Gauthier-Villar), 1891, p. 174—195);

(XV) M. Chasles: a) Note sur les propriétés générales du système de deux corps, Bull. de Férussac XIV, 321—326 (1830). b) Aperçu historique sur l'origine et le développement des méthodes en géométrie, Bruxelles, 1837.

(XVI) E. Galois, Œuvres mathématiques, Paris (Gauthier-Villars),1897.

(XVII) W. R. Hamilton, Lectures on Quaternions, Dublin, 1853.

(XVIII) A. Gayley, Collected Mathematical Papers, Cambridge, 1889—1898: a) On certain results relating to quaternions, т. I, стр. 123—126 (=Phil. Mag. (1845)); b) Sur les déterminants gauches, т. I, стр. 410—413 (=J. de Crelle XXXVIII (1848)); c) Recherches ultérieures sur les déterminants gauches, т. II, стр. 202—215 (=J. de Crelle L (1855)); d) A sixth memoir on quantics, т. II, стр. 561—592 (=Phil. Trans. (1859)).

(XIX) C. G. Jacobi, Gesammelte Werke, Berlin (G. Reimer), 1881—1891: a) Ueber die Pfaffsche Methode..., т. IV, стр. 17—29; b) Ueber einen algebraischen Fundamentalsatz und seine Anwendungen, т. III, стр. 593—598.

(XX) J. J. Sylvester, Collected Mathematical Papers, т. I, Cambridge, 1904: A demonstration of the theorem that every homogeneous quadratic polynomial is reducible by real orthogonal substitution to the form of a sum of positive and negative squares, стр. 378—381 (=Phil. Mag. (1852)).

(XXI) E. Laguerre, Œuvres, т. II, Paris (Gauthier-Villars), 1905.

(XXII) C. Hermite, Œuvres, т. I, Paris (Gauthier-Villars), 1905: Sur la théorie des formes quadratiques, стр. 200—263 (=J. de Crelle XLVII (1854)).

(XXIII) K. G. V. von Staudt, Beiträge zur Geometrie der Lage, Nürnberg, 1856.

(XXIV) E. Beltrami: a) Saggio di interpretazione della geometria non-euclidea, Giorn. Mat. VI, 284—312 (1868); b) Teoria fondamentale

degli spazii di cuvatura constante, Ann. Mat. (2) **II**, 232—255 (1868—1869).

(XXV) F. Klein, Gesammelte mathematische Abhandlungen, т. I, Berlin (Springer), 1921: a) Ueber die sogenannte Nicht-Euklidische Geometrie, стр. 254—305 (=Math. Ann. **IV** (1871)); b) Vergleichende Betrachtungen über neuere geometrische Forschungen, стр. 460—497 (=Math. Ann. **XLIII** (1893)).

(XXVI) C. Jordan, Traité des substitutions et des équations algébrigues, Paris (Gauthier-Villars), 1870.

(XXVII) G. Frobenius: a) Ueber lineare Substitutionen und bilineare Formen, J. de Crelle **LXXXIV**, 1—63 (1878); b) Theorie der linearen Formen mit ganzen Coeffizienten, J. de Crelle **LXXXVI**, 146—208 (1879).

(XXVIII) W. K. Clifford, Mathematical Papers, London (Macmillan), 1882: a) On the classification of geometric algebras, стр. 397—401; b) Applications of Grassmann's extensive algebras, стр. 266—276 (=Amer. J. Math. **I** (1878)).

(XXIX) R. Lipschitz, Untersuchungen über die Summen von Quadraten, Bonn, 1886.

(XXX) D. Hilbert, Grundlagen der Geometrie, Leipzig (Teubner), 1889.

(XXXI) E. Witt, Theorie der quadratischen Formen in beliebegen Körpern, J. de Crelle **CLXXVI**, 31—44 (1937).

(XXXII) E. Cartan, Leçons sur la théorie des spineurs, Actual Sci. et Industr. Paris (Hermann), 1938.

(XXXIII) C. L. Siegel, Symplectic Geometry, Amer. J. Math. **LXV**, 1—86 (1943).

(XXXIV) C. Chevalley, The algebraic theory of spinors, New York (Columbia Univ. Press), 1954.

(XXXV) M. Eichler, Quadratische Formen und orthogonale Gruppen, Berlin — Göttingen — Heidelberg (Springer), 1952.

УКАЗАТЕЛЬ ОБОЗНАЧЕНИЙ

	Глава	§	n°
$M(\alpha)$, M_α (M — модуль над кольцом A, α — элемент кольца A)	VII	2	1
$G(a)$ (a — целое >0) . .	VII	2	4
$m(p)$ (p^n — экстремальный элемент, n — целое $\geqslant 1$)	VII	4	7
E_u (u — эндоморфизм векторного пространства E)	VII	5	1
$U_{m,\alpha}$	VII	5	2
a_M, A_M (M — модуль над кольцом A, $a \in M$) . .	VIII	1	2
$\mathscr{L}_A(M)$ (M — модуль над A)	VIII	1	2
L_x, R_x (x — элемент кольца A)	VIII	1	2
A_r (A — кольцо)	VIII	1	2
$S(V)$, $S(f)$ $T(M)$, $T(g)$	VIII	1	4
$l_A(M)$, $[M:F]$ (M — полупростой A-модуль, F — простой A-модуль)	VIII	3	5
$\dim_D M$ (M — векторное пространство над D)	VIII	3	5
$[A:B]$, $i(A,B)$, $h(A,B)$ (A — простое кольцо, B — простое подкольцо в A с той же единицей)	VIII	5	6
UV, $\mathfrak{a}^n$ (U — подгруппа кольца A, V — подгруппа некоторого A-модуля, $\mathfrak{a}$ — идеал в A)	VIII	6	1
$\mathfrak{N}_A(M)$, $\mathfrak{N}(M)$ (M — A-модуль)	VIII	6	2
$\mathfrak{N}(A)$ (A — кольцо) . . .	VIII	6	3
(L,u,v), $u\cdot v$	VIII	8	1
$u_{(L)}$, $\mathfrak{F}_{(L)}$ (u — эндоморфизм векторного пространства V над K, $\mathfrak{F}$ — множество эндоморфизмов V, L — расширение поля K)	VIII	9	2
$\mathscr{B}(K)$	VIII	10	4
$\alpha\beta$, ε	VIII	10	4
α_L (α — элемент группы $\mathscr{B}(K)$, L — расширение поля K)	VIII	10	5
$\mathrm{Pc}_{M/K}(a, X)$, $\mathrm{N}_{M/K}(a)$, $\mathrm{Tr}_{M/K}(a)$, $\mathrm{Pc}_M(a; X)$, $\mathrm{N}_M(a)$, $\mathrm{Tr}_M(a)$ (a — элемент алгебры A над K, M — A-модуль) . . .	VIII	12	1
$\mathrm{Pc}_{A/K}(a; X)$, $\mathrm{N}_{A/K}(a)$, $\mathrm{Tr}_{A/K}(a)$, $\mathrm{Pc}(a; X)$, $\mathrm{N}(a)$, $\mathrm{Tr}(a)$ (A — алгебра над K, $a \in A$) . . .	VIII	12	2
$\mathrm{Pcrd}_{A/K}(x; X)$, $\mathrm{Nrd}_{A/K}(x)$, $\mathrm{Trd}_{A/K}(x)$, $\mathrm{Pcrd}(x; X)$, $\mathrm{Nrd}(x)$, $\mathrm{Trd}(x)$ (A — простая центральная алгебра над K, $x \in A$)	VIII	12	3
$\mathrm{Pc}(X_1, \ldots, X_m; X)$, $\mathrm{N}(X_1, \ldots, X_m)$, $\mathrm{Tr}(X_1, \ldots, X_m)$ . . .	VIII	12	3
$\mathrm{Pcrd}(X_1, \ldots, X_m; X)$, $\mathrm{Nrd}(X_1, \ldots, X_m)$, $\mathrm{Trd}(X_1, \ldots, X_m)$ . .	VIII	12	3

	Глава	§	n°
$\varrho_1+\varrho_2+\ldots+\varrho_n$ (ϱ_i — линейные представления)	VIII	13	1
$\varrho_{(L)}$ (ϱ — линейное представление некоторой алгебры над K, L — расширение поля K)	VIII	13	4
$\mathrm{Pc}_\rho(x; X)$, $\mathrm{N}_\rho(x)$, $\mathrm{Tr}_\rho(x)$ (ϱ — линейное представление)	VIII	13	5
$\widetilde{A}$, $\widetilde{\mathfrak{a}}$ (A — алгебра без единицы, $\mathfrak{a}$ — идеал в A)	VIII	Прилож.	1
$\mathfrak{R}(A)$ (A — алгебра без единицы)	VIII	Прилож.	3
d_Φ, s_Φ	IX	1	1 и 6
b^j, $b^{j'}$	IX	1	2
F^J (J — антиавтоморфизм кольца скаляров B правого A-модуля F)	IX	1	2
N^0, M^0 (N, M — подмодули)	IX	1	3
$\hat{\Phi}$	IX	1	7
u^* (u — гомоморфизм)	IX	1	8
$\Phi_{(m)}$	IX	1	9
$M(x)$ (x — элемент свободного модуля)	IX	1	10
$M(u)$ (u — гомоморфизм свободного модуля в свободный модуль)	IX	1	10
${}^tM$, M^J (M — матрица)	IX	1	10
$D_\Phi(x_1, \ldots, x_n)$, $D_\Phi(S)$	IX	2	
$\bar{\alpha}$ (α — скаляр)	IX	3	
$Pf(R)$	IX	5	2
$\mathrm{Sp}(\Phi)$, $\mathrm{Sp}(2m, A)$, $\mathrm{Sp}_{2m}(A)$	IX	5	3
$\boldsymbol{U}(\Phi)$, $\boldsymbol{SU}(\Phi)$ (Φ — эрмитова форма)	IX	6	2
$\boldsymbol{O}(Q)$, $\boldsymbol{SO}(Q)$ (Q — квадратичная форма)	IX	6	2
$\boldsymbol{U}(n, A)$, $\boldsymbol{SU}(n, A)$, $\boldsymbol{O}(n, A)$, $\boldsymbol{SO}(n, A)$	IX	6	2
$Q \top Q'$, $Q \sim Q'$ (Q, Q' — квадратичные формы)	IX	8	1
$\vartheta(Q)$ (Q — квадратичная форма)	IX	8	1
$T+T'$, $a \cdot T$ (T, T' — типы квадратичных форм)	IX	8	2
$\delta(Q)$ (Q — квадратичная форма)	IX	8	2
$Q \otimes Q'$ (Q, Q' — квадратичные формы)	IX	8	3
TT' (T, T' — типы квадратичных форм)	IX	8	3
T^h, T^+, T^-	IX	9	1
$C(Q)$, $I(Q)$, ϱ_Q, ϱ, $C^+(Q)$, $C^-(Q)$, C^+, C^- (Q — квадратичная форма)	IX	9	1
α, β, $C(f)$	IX	9	1
e_x, i_f, i_x^F, λ_F	IX	9	2
$\bar{\lambda}_F$	IX	9	3
G, G^+, G_0^+, $O^+(Q)$, $O_0^+(Q)$, $N(s)$ (Q — квадратичная форма, s — обратимый элемент специальной группы Клиффорда G^+)	IX	9	5
$A(\Phi)$ (Φ — симметрическая билинейная форма на векторном пространстве размерности 2)	IX	10	1
S, S^+, H, O^+	IX	10	1
$\bar{u}$ (u — прямое подобие), i, d	IX	10	1
c_w, s_w, t_w, c, s, t	IX	10	2
H^+	IX	10	3
$(\widehat{D_1, D_2})$ (D_1, D_2 — прямые или полупрямые)	IX	10	3
$\mathfrak{A}_1$, $\mathfrak{A}_0$, h, h'	IX	10	3
$\|x\|$, $(\widehat{x, y})$ (x, y — векторы)	IX	10	3
$\cos\vartheta$, $\sin\vartheta$, $\mathrm{tg}\,\vartheta$, $\mathrm{ctg}\,\vartheta$	IX	10	3
$]D_1, D_2[$, $[D_1, D_2]$ (D_1, D_2 — полупрямые в ориентированной плоскости)	IX	10	4

УКАЗАТЕЛЬ ТЕРМИНОВ

	Глава	§	n°
Абсолютно неприводимое линейное представление	VIII	13	4
— *полупростая алгебра*	VIII	7	5
— *полупростое линейное представление*	VIII	13	5
— — *множество эндоморфизмов*	VIII	9	2
— — *семейство эндоморфизмов*	VIII	9	2
— *полупростой модуль*	VIII	7	5
— — *эндоморфизм*	VIII	9	2
— *простое линейное представление*	VIII	13	4
Автоморфизм главный	VII	2	2
— — *алгебры Клиффорда*	IX	9	1
— *ортогональный*	IX	6	2
— — *от n переменных*	IX	6	2
— *симплектический*	IX	5	3
— — *от 2m переменных*	IX	5	3
— *унитарный*	IX	6	2
— — *от n переменных*	IX	6	2
Алгебра абсолютно полупростая	VIII	7	5
— *алгебраическая*	VIII	11, упр.	1
— *Клиффорда*	IX	9	1
— — *квадратичной формы*	IX	9	1
—, *нейтрализующаяся некоторым расширением поля скаляров*	VIII	10	5
— *простая центральная*	VIII	5	4
— *сепарабельная*	VIII	7	5
Аннулирующийся элемент	VII	2	1
Антиавтоморфизм главный алгебры Клиффорда	IX	9	1
Антиавтоморфизм кольца	IX	1	2
Антисимметрическая матрица	IX	3	1
Антиэрмитова матрица	IX	3	1
— *форма*	IX	3	1
Артинов модуль	VIII	2	1
Артиново кольцо	VIII	2	3
Ассоциированная билинейная форма (с квадратичной формой)	IX	3	4
Ассоциированное линейное отражение (с билинейным отображением)	IX	1	1
— *полулинейное отображение* (с полуторалинейной формой)	IX	1	6
Аффинная квадрика	IX	6, упр.	25
— — *вырожденная*	IX	6, упр.	25
— *коника*	IX	6, упр.	25
— — *вырожденная*	IX	6, упр.	25
Аффинные сопряженные линейные многообразия	IX	6, упр.	25
Базис ортогональный	IX	6	1
— *ортонормальный*	IX	6	1
— *симплектический*	IX	5	1
Бернсайда теорема	VIII	4	3
Безу тождество	VII	1	2
Бикоммутант кольца	VIII	1	2
— *модуля*	VIII	1	2
Билинейная форма	IX	1	6
— —, *ассоциированная с квадратичной формой*	IX	3	4
— — *эрмитова*	IX	3	1
Билинейное отображение	IX	1	1

	Глава	§	n°
Билинейное отображение, вырожденное справа (слева)	IX	1	1
— — *невырожденное*	IX	1	1
— — —, *ассоциированное с билинейным отображением*	IX	1	3
— —, *полученное расширением скаляров*	IX	1	4
Бимодуль	IX	1	1
Брауэра группа	VIII	10	4
Веддерберна теорема	VIII	11	1
Вектор, ортогональный к линейному многообразию	IX	6	6
— *собственный эндоморфизма*	VII	5	3
— — *квадратной матрицы*	VII	5	3
Вектора длина	IX	10	3
Витта группа	IX	8	2
— *кольцо*	IX	8	3
— *разложение*	IX	8	2
— *теорема*	IX	4	3
Внешняя прямая сумма квадратичных форм	IX	3	4
— — — *квадратических модулей*	IX	3	4
Вполне изотропный подмодуль	IX	4	1
— *ортогональное многообразие* (к линейному многообразию)	IX	1	6
— *ортогональный подмодуль* (к подмодулю)	IX	1	3
— *приводимое линейное представление*	VIII	13	1
— *сингулярный подмодуль*	IX	4	1
Вращение	IX	9	5
Вырожденная квадрика аффинная	IX	6, упр.	25
— — *проективная*	IX	6, упр.	23
— *коника аффинная*	IX	6, упр.	25
Вырожденная коника проективная	IX	6, упр.	23
Вырожденное (справа, слева) билинейное отображение	IX	1	1
— (—, —) *полуторалинейное отображение*	IX	1	2
Высота простого кольца над простым подкольцом	VIII	5	6
Гамильтона — Кэли теорема	VII	5	3
	VII	22	
Гиперплоскость радикальная двух сфер	IX	10, упр.	12
Главный автоморфизм алгебры Клиффорда	IX	9	1
— *антиавтоморфизм алгебры Клиффорда*	IX	9	1
Главных идеалов наибольший общий делитель	VII	1	2
— — *кольцо*	VII	1	1
Гомоморфизм канонический алгебры Клиффорда	IX	9	1
— — *алгебры* $\mathscr{L}_A(M) \otimes_K B'$ *в алгебру* $\mathscr{L}_B(M)$	VIII	10	2
— — *бикоммутанта в бикоммутант прямого множителя*	VIII	1	3
— — *модуля* V *в модуль* $T(S(V))$	VIII	1	4
— — — $S(T(M))$ *в модуль* M	VIII	1	4
— *метрический*	IX	4	3
— *подмодуля модуля* E *в алгебру Клиффорда модуля* E	IX	9	1
— *сопряженный (слева, справа)*	IX	1	8
Грама — Шмидта процесс ортогонализации	IX	6	1
Группа Брауэра	VIII	10	4

	Глава	§	n°
Группа Витта	IX	8	2
— *вращений*	IX	9	5
— *Галуа*	VIII	10 упр.	6
— *Клиффорда*	IX	9	5
— — *приведенная*	IX	9	5
— — *специальная*	IX	9	5
— *конформная*	IX	10 упр.	14
— *кручения*	VII	2	2
— *ортогональная, ассоциированная с Q*	IX	6	2
— — *от n переменных*	IX	6	2
— — *специальная*	IX	6	2
— *симплектическая, ассоциированная с Ф*	IX	5	3
— — *от 2m переменных*	IX	5	3
— *типов квадратичных форм*	IX	8	2
— *унитарная, ассоциированная с Ф*	IX	6	2
— — *от n переменных*	IX	6	2
— — *специальная*	IX	6	2
Делители модуля элементарные	VII	4	7
Диагонализируемое множество эндоморфизмов	VIII	9	3
— *семейство эндоморфизмов*	VIII	9	3
Диагонализируемый эндоморфизм	VIII	9	3
Диксона инвариант	IX	9 упр.	9
Дискриминант полуторалинейной формы относительно системы элементов	IX	2	2
Длина вектора	IX	10	3
— *линейного представления*	VIII	13	1
— *полупростого модуля*	VIII	3	5
Евклидово пространство	IX	6	6
Единица правая (левая) по модулю идеала	VIII	Прилож.	1
Единичная окружность	IX	10 упр.	2
Закон инерции	IX	7	2
Замкнутая полупрямая	IX	10	3
Замкнутый угловой сектор	IX	10	4
Знакопеременная матрица	IX	3	1
Значение собственное квадратной матрицы	VII	5	3
— — *эндоморфизма*	VII	5	3
Идеал минимальный	VIII	3	1
— *нильпотентный*	VIII	6	1
— *примитивный*	VIII	8 упр.	5
— *регулярный*	VIII	Прилож.	1
Изоморфные композиции расширений	VIII	8	1
— *линейные представления*	VIII	13	1
Изотипная компонента полупростого модуля	VIII	3	4
Изотипный модуль	VIII	1	3
Изотропная полупрямая	IX	10	3
Изотропное линейное многообразие	IX	6	6
Изотропный вполне подмодуль	IX	4	1
— *конус*	IX	6 упр.	23
— *подмодуль*	IX	4	1
— *элемент*	IX	4	1
Инвариант Диксона	IX	9 упр.	9
Инвариантные множители линейного отображения	VII	4	5
— — *матрицы*	VII	4	5
— — *модуля конечного типа*	VII	4	3
— — *подмодуля свободного модуля относительно*	VII	4	2
Инварианты подобия эндоморфизма	VII	2	2
	VII	5	1
— — *квадратной матрицы*	VII	5	1

	Глава	§	n°
Инверсия сферы	IX	10	упр. 13
Инволюция в линейной группе	IX	6	3
Индекс квадратичной формы	IX	4	2
— *полуторалинейной формы*	IX	4	2
— *простого подкольца в простом кольце*	VIII	5	6
Канонический гомоморфизм алгебры Клиффорда	IX	9	1
— — — $\mathscr{L}_A(M) \otimes_K B'$ *в алгебру* $\mathscr{L}_B(M)$	VIII	10	2
— — *бикоммутанта в бикоммутант прямого множителя*	VIII	1	3
— — *модуля V в модуль* $T(S(V))$	VIII	1	4
— — — $S(T(M))$ *в модуль* M	VIII	1	4
Каноническое отображение множества эрмитовых эндоморфизмов на множество эрмитовых форм	IX	7	3
— — — $\mathfrak{A}$ *на* S^+/H	IX	10	3
— — — $\mathfrak{A}$ *на* O^+	IX	10	3
— — — $\mathscr{L}_C(V, V')$ *в* $\mathscr{L}_A(S(V), S(V'))$	VIII	1	4
— — — $\mathscr{L}_A(M, M')$ *в* $\mathscr{L}_C(T(M), T(M'))$	VIII	1	4
— — *модуля в его алгебру Клиффорда*	IX	9	1
— *разложение модуля кручения на компоненты*	VII	2	2
Касательное линейное многообразие к квадрике	IX	6	упр. 23, 25
Квадратический модуль	IX	3	4
Квадратичная форма	IX	1	4
— — *невырожденная*	IX	3	4
— — *нейтральная*	IX	8	1
Квадратичная форма положительная (отрицательная)	IX	7	1
— —, *полученная расширением скаляров*	IX	3	4
Квадратичные формы эквивалентные	IX	1	6
Квадрика аффинная	IX	6	упр. 25
— *проективная*	IX	6	упр. 23
Квазиобратный элемент (правый, левый)	VIII	Прил.	3
Класс простого A-модуля	VIII	3	2
— *простой центральной алгебры*	VIII	7	4
Клиффорда алгебра	IX	9	1
— — *квадратичной формы*	IX	9	1
— *группа*	IX	9	5
— — *приведенная*	IX	9	5
— — *специальная*	IX	9	5
Кольцо артиново (слева, справа)	VIII	2	3
— *Витта*	IX	8	3
— *вполне примарное*	VIII	6,	упр. 20
— *Галуа*	VIII	10,	упр. 5
— — *слабое*	VIII	10,	упр. 5
— *главных идеалов*	VII	1	1
— *гомотетий некоторого модуля*	VIII	1	2
— *инволютивное*	VIII	2,	упр. 11
— *квазипростое*	VIII	5,	упр. 5
— *нетерово (слева, справа)*	VIII	2	3
— *полупростое*	VIII	5	1
— *примарное*	VIII	6,	упр. 20
— *примитивное (слева)*	VIII	5,	упр. 5
— *простое*	VIII	5	2
— *регулярное*	VIII	6,	упр. 15
— *типов квадратичных форм*	IX	8	3
— *фробениусово*	VIII	4,	упр. 10
Коммутант кольца	VIII	1	2
— *модуля*	VIII	1	3

	Глава	§	n°
Комплекс линейный	IX	10, упр.	16
Композиция расширений	VIII	8	1
Компонента изотипная полупростого модуля	VIII	3	4
— неприводимая матричного представления	VIII	13	2
— нильпотентная эндоморфизма	VIII	9	4
— полупростая эндоморфизма	VIII	9	4
— простая полупростого кольца	VIII	5	3
Коника аффинная	IX	6, упр.	25
— — вырожденная	IX	6, упр.	25
— проективная	IX	6, упр.	23
— — вырожденная	IX	6, упр.	23
Контрмодуль модуля	VIII	1	2
Конформная группа	IX	10, упр.	14
Корегулярное представление	VIII	13	1
Косинус (функция)	IX	10	3
— угла	IX	10	3
Котангенс (функция)	IX	10	3
— угла	IX	10	3
Коэффициент линейного представления	VIII	13	3
— подобия	IX	6	5,6
Кратность элементарного делителя	VII	4	7
Кручения группа	VII	2	2
— модуль	VII	2	1
— подмодуль	VII	2	2
Лагерра формула	IX	10, упр.	25
Лемма Накаяма	IX	6	3
— Шура	IX	4	3
Линейное многообразие изотропное	IX	6	6
— —, касательное к квадрике	IX	6, упр.	23, 25
— отображение, ассоциированное справа (слева) с билинейным отображением	IX	1	1
Линейное представление	VIII	13	1
— — абсолютно неприводимое	VIII	13	4
— — — полупростое	VIII	13	4
— — — простое	VIII	13	4
— — алгебры	VIII	13	1
— —, ассоциированное с A-модулем	VIII	13	1
— — вполне приводимое	VIII	13	1
— — группы	VIII	13	1
— — корегулярное	VIII	13	1
— — неприводимое	VIII	13	1
— — полупростое	VIII	13	1
— — —, содержащее n раз некоторое простое представление	VIII	13	1
— —, полученное расширением поля скаляров	VIII	13	1
— — простое	VIII	13	1
— — регулярное	VIII	13	1
— — точное	VIII	13	1
— — транспонированное	VIII	13	1
— факторпредставление	VIII	13	1
Линейные многообразия перпендикулярные	IX	6, упр.	22
— представления изоморфные	VIII	13	1
— — подобные	VIII	13	1
Линейный комплекс	IX	10, упр.	16
Максимальный подмодуль	VIII	3	1
Матрица антисимметрическая	IX	3	1
— антиэрмитова	IX	3	1
— билинейного отображения	IX	1	1
— жорданова	VII	5	2
— знакопеременная	VII	3	1
— линейного отображения, удовлетворяющего условиям (Л), (П), (ЛП), (ПЛ)	IX	1	10
— нормальная	IX	7, упр.	17
— ортогональная	IX	6	2

	Глава	§	n°
Матрица полуторалинейного отображения	IX	1	2
— *симметрическая*	IX	3	1
— *симплектическая*	IX	7	3
— *унитарная*	IX	6	2
— *эрмитова*	IX	3	1
Матричное представление	VIII	13	2
Метрическая форма	IX	6	6
Метрический гомоморфизм	IX	6	6
	IX	4	3
Минимальный идеал	VIII	3	1
— *многочлен эндоморфизма*	VII	5	1
Многочлен минимальный элемента алгебры	VIII	11, упр.	1
— *характеристический* (см. *Характеристический многочлен*)			
Множество классов простых A-модулей	VIII	3	2
— *абсолютное простое эндоморфизмов*	VIII	9	2
— *диагонализируемое эндоморфизмов*	VIII	9	3
— *полупростое эндоморфизмов*	VIII	9	1
Модуль абсолютно полупростой	VIII	7	5
— *артинов*	VIII	2	1
— *без кручения*	VIII	2	1
— *изотипный*	VIII	1	3
— *квадратический*	IX	3	4
— *конечного типа*	VII	22	2
— *конечной длины*	VIII	2	1
— *кручения*	VII	2	1
— *линейного представления*	VIII	13	1
— *над алгеброй*	VIII	Прилож.	2
— *неразложимый*	VII	4	7
— *нетеров*	VIII	2	1
— *полупростой*	VIII	3	3
— *простой*	VIII	3	1
	и Прилож.		2

	Глава	§	n°
Модуль разложимый	VII	4	7
— *сепарабельный*	VIII	7	5
Наибольший общий делитель (н. о. д.) *главных идеалов*	VII	1	2
Накаяма лемма	VIII	6	3
Невырожденная квадратичная форма	IX	3	4
Невырожденное билинейное отображение	IX	1	1
— — —, *ассоциированное с билинейным отображением*	IX	1	3
— *полуторалинейное отображение*	IX	1	2
— — —, *ассоциированное с полуторалинейным отображением*	IX	1	3
— *справа (слева) полуторалинейное отображение*	IX	1	2
Нейтрализующаяся алгебра	VIII	10	5
Нейтрализующее поле	VIII	10	5
— *расширение*	VIII	10	5
Нейтральная квадратичная форма	IX	8	1
— *полуторалинейная форма*	IX	4	2
Неприводимая компонента матричного представления	VIII	13	2
Неприводимое линейное представление	VIII	13	1
Нетеров модуль	VIII	2	1
Нетерово кольцо	VIII	2	3
Нечетный элемент алгебры Клиффорда	IX	9	1
Нильидеал	VIII	6	1
Нильпотентный идеал	VIII	6	1
— *элемент*	VIII	6	1
— *эндоморфизм*	VII	5	2
Норма в алгебре	VIII	12	2
— *относительно линейного представления*	VIII	13	5

	Глава	§	n°
Норма относительно модуля	VIII	12	1
— *приведенная*	VIII	12	3
— *спинорная*	IX	9	5
Нормальная матрица	IX	7, упр.	17
Нормальный эндоморфизм	IX	7	3
Образ гомоморфизма	VIII	1	1
Обратимый (справа, слева) элемент	VIII	6	3
Обратная форма	IX	1	7
Обратный образ билинейного отображения	IX	1	1
— — *полуторалинейного отображения*	IX	1	1
— — *правый (левый)*	VIII	6	3
Окружность единичная	IX	10, упр.	2
Ориентация пространства	IX	10	3
Ориентированное пространство	IX	10	3
Ортогонализация (процесс Грама — Шмидта)	IX	6	1
Ортогональная группа	IX	6	2
— —, *ассоциированная с Q*	IX	6	2
— — *от n переменных*	IX	6	2
— — *специальная*	IX	6	2
— *матрица*	IX	6	2
— *проекция на линейное многообразие*	IX	6	6
Ортогональное многообразие (к линейному многообразию)	IX	6	6
— *преобразование*	IX	6	2
— *проектирование*	IX	6	3
— — *на линейное многообразие*	IX	6	6
— *семейство идемпотентов*	IX	1	1
— — *проектирований*	IX	1	1
Ортогональные линейные многообразия	IX	6	6
— — *подмножества*	IX	1	3
Ортогональные слабо подпространства	IX	3, упр.	11
— *сферы*	IX	10, упр.	12
— *элементы* (относительно квадратичной формы)	IX	1	3
	IX	3	4
— — (— полуторалинейного отображения)	IX	1	3
Ортогональный автоморфизм	IX	6	2
— *базис*	IX	6	1
— *вектор* (к линейному многообразию)	IX	6	6
— *подмодуль* (к подмодулю)	IX	1	3
Основание цоколя	VIII	5, упр.	9
Ось аффинного линейного комплекса	IX	10, упр.	16
Открытая полупрямая	IX	10	3
Открытый угловой сектор	IX	10	4
Отображение билинейное (см. *Билинейное отображение*)			
— *каноническое* (см. *Каноническое отображение*)			
— *линейное* (см. *Линейное отображение*)			
— *полулинейное* (см. *Полулинейное отображение*)			
— *полуторалинейное* (см. *Полуторалинейное отображение*)			
Отрицательная эрмитова форма	IX	7	1
— *квадратичная форма*	IX	7	1
Отрицательный n-вектор	IX	10	3
Перемещение	IX	6	6
Перпендикулярные линейные многообразия	IX	6, упр.	22
Пифагора теорема	IX	6	6
Плотное подкольцо	IX	4	2
Плотности теорема	IX	4	2

	Глава	§	n°
Подмножества ортогональные	IX	1	3
Подмодуль вполне изотропный	IX	4	1
— — *ортогональный* (к подмодулю)	IX	1	3
— — *сингулярный*	IX	4	1
— *изотропный*	IX	4	1
— *кручения*	VII	2	1
— *максимальный*	IX	3	1
— *модуля над алгеброй*	VIII	Прилож.	2
— *ортогональный* (к подмодулю)	IX	1	3
— *сингулярный*	IX	4	1
Подобие	IX	6	5,6
— *обратное*	IX	6	5
— *прямое*	IX	9,	упр. 9
Подобные алгебры	VIII	10	4
— *линейные представления*	VIII	13	1
— *эндоморфизмы*	VII	5	1
Подпредставление линейного представления	VII	13	1
Подпространства слабо ортогональные	IX	3,	упр. 11
Подпространство собственное	VII	5	3
— *эндоморфизма*	VII	5	3
Поле рефлексивное	IX	11,	упр. 4
Положительная квадратичная форма	IX	7	1
— *эрмитова форма*	IX	7	1
Положительный n-вектор	IX	10	3
Полулинейное отображение, ассоциированное с полуторалинейной формой	IX	1	6
— —, — *справа (слева) с полуторалинейной формой*	IX	1	6
— — *сопряженное*	IX	7	3
Полупростая компонента эндоморфизма	VIII	9	4
Полупростое кольцо	VIII	5	1
— *линейное представление*	VIII	13	1
— *множество эндоморфизмов*	VIII	9	3
— *семейство эндоморфизмов*	VIII	9	3
Полупростой модуль	VIII	9	3
— *эндоморфизм*	VIII	9	1
Полупрямая	IX	10	3
— *замкнутая*	IX	10	3
— *изотропная*	IX	10	3
— *открытая*	IX	10	3
Полуторалинейная форма	IX	1	6
— — *нейтральная*	IX	1	6
Полуторалинейное отображение	IX	1	2
— — *невырожденное (справа, слева)*	IX	1	2
— — —, *ассоциированное с полуторалинейным отображением*	IX	1	3
— —, *полученное расширением скаляров*	IX	1	4
— *справа (слева) отображение* (относительно антиавтоморфизма)	IX	1	2
Полуспинор	IX	9	4
Полуторалинейные формы эквивалентные	IX	1	6
Полюс гиперплоскости относительно квадрики	IX	6,	упр. 23, 25
— *инверсии*	IX	10,	упр. 12
Поляра линейного многообразия относительно квадрики	IX	6,	упр. 23, 25
Последовательность прямая полупрямых	IX	10	4
Представление линейное (см. *Линейное представление*)			
— *матричное*	VIII	13	2
Представления спинорные	IX	9	4

	Глава	§	n°
Преобразование ортогональное	IX	6	2
— *симплектическое*	IX	5	3
— *унитарное*	IX	6	2
Приведенная группа Клиффорда	IX	9	5
— *норма*	VIII	12	3
Приведенный след	VIII	12	3
— *характеристический многочлен*	VIII	12	3
Приводимый к диагональному виду эндоморфизм	VII	5	4
Присоединение единицы	VIII	Прилож.	1
Продолжение полуторалинейной формы на внешнюю степень	IX	1	9
— — — *на тензорную степень*	IX	1	9
Проективная квадрика	IX	6, упр.	23
— *коника*	IX	6, упр.	23
Проектирование	VIII	1	1
— *модуля M на модуль N*	VIII	1	1
— *ортогональное*	IX	6	3
— — *на линейное многообразие*	IX	6	6
Проекция ортогональная на линейное многообразие	IX	6	6
— *стереографическая*	IX	10, упр.	14
Произведение подгрупп	VIII	6	1
— *тензорное квадратичных форм*	IX	8	3
— — *полуторалинейных форм*	IX	1	9
Простая компонента полупростого кольца	VIII	5	3
Простое кольцо	VIII	5	2
— *линейное представление*	VIII	13	1
Простой модуль	VIII	3	1
	VIII	Прилож.	2
Пространство определения квадратичной формы	IX	8	1
Пространство ориентированное	IX	6	6
— *евклидово*	IX	6	6
— *эрмитово*	IX	6	6
Процесс ортогонализации Грама — Шмидта	IX	6	1
Прямая последовательность полупрямых	IX	10	4
— *с отмеченной точкой*	IX	10, упр.	2
— *сумма билинейных (полуторалинейных) отображений*	IX	1	3
— — *внешняя квадратичных форм (квадратических модулей)*	IX	3	4
— — *линейных представлений*	IX	13	1
Прямое подобие	IX	6	5
Прямой множитель модуля	IX	1	1
— *угол*	IX	10	3
Псевдодискриминант	IX	9, упр.	9
Пфаффиан знакопеременной матрицы	IX	5	2
Радикал алгебры	VIII,	Прилож.	3
— *кольца*	VIII	6	3
— *модуля*	VIII	6	2
Радиус сферы	IX	10, упр.	12
Развернутый угол	IX	10	3
Разложение Витта	IX	4	2
— *каноническое модуля кручения на компоненты*	VII	2	2
— *элемента на экстремальные множители*	VII	1	3
Разложимый модуль	VII	4	7
Размерность векторного пространства	VIII	3	5
— *квадратичной формы*	IX	8	1
Ранг билинейной (полуторалинейной) формы	IX	1	6
— *модуля без кручения*	VII	3	1
Расстояние	IX	7	1

	Глава	§	n°
Расширение нейтрализующее	IX	10	5
Сектор угловой	IX	10, упр.	18
— — *замкнутый*	IX	10	4
— — *открытый*	IX	10	4
— — *развернутый*	IX	10, упр.	8
Семейство абсолютно простое эндоморфизмов	VIII	9	2
— *диагонализируемое эндоморфизмов*	VIII	9	3
— *ортогональное идемпотентов*	VIII	1	1
— — *проектирований*	VIII	1	1
— *полупростое эндоморфизмов*	VIII	9	1
Сепарабельная алгебра	VIII	7	5
Сепарабельный модуль	VIII	7	5
Сигнатура эрмитовой формы	IX	7	2
Симметрическая матрица	IX	3	1
Симметрия относительно аффинного линейного многообразия	IX	6	6
— — *векторного подпространства*	IX	6	3
— — *гиперплоскости*	IX	6	4
Симплектическая группа	IX	5	3
— —, *ассоциированная с* Ф	IX	5	3
— — *от* 2*m переменных*	IX	5	3
— *матрица*	IX	5	3
Симплектический автоморфизм	IX	5	3
— — *от* 2*m переменных*	IX	5	3
— *базис*	IX	5	1
Симплектическое преобразование	IX	5	3
Синус (функция)	IX	10	3
— *угла*	IX	10	3
Сингулярный вполне подмодуль	IX	4	1
— *подмодуль*	IX	4	1
— *элемент*	IX	4	1
Система представителей экстремальных элементов	VII	1	3
Сколема—Нетер теорема	VIII	10	1
След в алгебре	VIII	12	2
— *модуля*	VIII	12	3
— *относительно линейного представления*	VIII	12	1
— *приведенный*	VIII	12	3
Собственное векторное подпространство	VII	5	3
— — — *эндоморфизма*	VII	5	3
— *значение*	VII	5	3
— *подпространство*	VII	5	3
Собственный вектор	VII	5	3
Соотношение Шаля	IX	10	3
Сопряженное полулинейное отображение	IX	7	3
Сопряженные аффинные линейные многообразия	IX	6, упр.	25
— *проективные линейные многообразия*	IX	6, упр.	23
Сопряженный (*слева, справа*) *гомоморфизм*	IX	1	8
Специальная унитарная группа	IX	6	2
Спинор	IX	9	4
Спинорная норма	IX	9	5
Спинорные представления	IX	9	4
Степень идеала	VIII	6	1
— *инверсии*	IX	10, упр.	13
— *кольца над простым подкольцом*	VIII	5	6
— *линейного представления*	VIII	13	1
— *точки относительно сферы*	IX	10, упр.	18
Стереографическая проекция	IX	10, упр.	14
Сфера	IX	10, упр.	12
Сферы ортогональные	IX	10, упр.	12
Тангенс (функция)	IX	10	3
— *угла*	IX	10	3

	Глава	§	n°
Тензорное произведение квадратичных форм	IX	8	3
— — *полуторалинейных форм*	IX	1	9
Теорема Бернсайда	VIII	4	3
— *Веддерберна*	VIII	1	1
— *Витта*	IX	4	3
— *Гамильтона — Кэли*	VII	5	3
	VII	2	2
— *Пифагора*	IX	6	6
— *плотности*	VIII	4	2
— *Сколема — Нетер*	VIII	10	1
— *Фробениуса*	VIII	11	2
— *Шаля*	IX	10	3
Тип квадратичной формы	IX	8	1
Тождество Безу	VII	12	
Точка обзора стереографической проекции	IX	10, упр.	14
Точное линейное представление	VIII	13	1
Транспонированное линейное представление	VIII	13	1
Тригонометрическая функция	IX	10	3
Угол вращения	IX	10	3
— *между двумя векторами в плоскости*	IX	10	3
— — — — *в пространстве размерности* $n \geqslant 2$	IX	10	3
— — — *полупрямыми*	IX	10	3 и упр. 6
— — — — *в аффинной плоскости*	IX	10	3
— — — *прямыми*	IX	10	3 и упр. 2
— — — — *в аффинной плоскости*	IX	10	3
— — — — *с отмеченными точками*	IX	10, упр.	2
— *прямого подобия*	IX	10, упр.	6
— *прямой*	IX	10	3 и упр. 2
— *развернутый*	IX	10	3 и упр. 6
Умножение правое (левое)	VIII	1	2
Унитарная группа	IX	6	2
Унитарная группа, ассоциированная с Ф	IX	6	2
— — *от n переменных*	IX	6	2
— — *специальная*	IX	6	2
— *матрица*	IX	6	2
Унитарное преобразование	IX	6	2
Унитарный автоморфизм	IX	6	2
— — *от n переменных*	IX	6	2
Условие (C)	IX	6	1
— (C′)	IX	6	1
— (T)	IX	4	2
Факторпредставление линейное	VIII	13	1
Форма антиэрмитова	IX	1	3
— *билинейная*	IX	1	6
— —, *ассоциированная с квадратичной формой*	IX	3	4
— — *эрмитова*	IX	3	1
— *квадратичная*	IX	1	4
— — *невырожденная*	IX	3	4
— — — *положительная (отрицательная)*	IX	7	1
— —, *полученная расширением скаляров*	IX	3	4
— *метрическая*	IX	6	6
— *нейтральная*	IX	4	2
	IX	8	1
— — *квадратичная*	IX	8	1
— — *полуторалинейная*	IX	4	2
— *обратная* (к билинейной (полуторалинейной форме)	IX	1	7
— *полуторалинейная*	IX	1	6
— *эрмитова*	IX	3	1
— — *положительная (отрицательная)*	IX	7	1
— *ε-эрмитова*	IX	3	1
Формула Лагерра	IX	10, упр.	5
Формы квадратичные эквивалентные	IX	3	4
— *полуторалинейные эквивалентные*	IX	1	6

	Глава	§	n°
Фробениуса теорема	VIII	11	2
Функция косинус	IX	10	3
— *котангенс*	IX	10	3
— *синус*	IX	10	3
— *тангенс*	IX	10	3
— *тригонометрическая*	IX	10	3
Характеристический многочлен в алгебре	VIII	12	2
— — *квадратной матрицы*	VII	5	3
— — *относительно линейного представления*	VIII	12	5
— — — *модуля*	VIII	2	1
— — *приведенный*	VIII	12	3
— — *эндоморфизма*	VII	5	3
Центр квадрики	IX	6, упр. 25	
	IX	10, упр. 12	
Централизатор кольца	VIII	1	2
Центральная простая алгебра	VIII	5	4
Цоколь правый (левый) кольца	IX	10, упр. 5	
Четный элемент алгебры Клиффорда	IX	9	1
Шаля соотношение	IX	10	3
— *теорема*	IX	10	3
Шура лемма	VIII	4	3
Эквивалентные квадратичные формы	IX	3	4
— *полуторалинейные формы*	IX	1	6
Элемент, аннулирующийся элементом	VII	2	1
— *без кратных множителей*	VIII	6	3
— *изотропный*	IX	4	1
Элемент обратимый (справа, слева)	VIII	6	3
— *нечетный алгебры Клиффорда*	IX	9	1
— *нильпотентный*	VIII	6	1
— *сингулярный*	IX	9	1
— *четный алгебры Клиффорда*	IX	9	1
Элементы ортогональные	IX	1	3
— — *относительно квадратичной формы*	IX	3	4
— — *полуторалинейного отображения*	IX	1	3
Эндоморфизм абсолютно полупростой	VIII	9	2
— *диагонализируемый*	VIII	9	3
— *нильпотентный*	VII	5	2
— *нормальный*	IX	7	3
— *полупростой*	IX	9	1
—, *приводимый к диагональному виду*	VII	5	4
— *эрмитов*	IX	7	3
Эндоморфизмы подобные	VII	5	1
— *эквивалентные*	VII	Прилож.	2
Эрмитов эндоморфизм	IX	7	3
Эрмитова матрица	IX	3	1
— *форма*	IX	3	1
— — *отрицательная*	IX	7	1
— — *положительная*	IX	7	1
Ядро квадратического модуля	IX	3	4
$\tilde{A}$-модуль, ассоциированный с A-модулем	VIII	Прилож.	2
p-вектор отрицательный	IX	10	3
— *положительный*	IX	10	3
p-группа	VII	2	2
ε-эрмитова матрица	IX	3	1
— *форма*	IX	3	1
π-компонента модуля	VII	2	2